

Nasa CR 65254

# AES-EPO STUDY PROGRAM

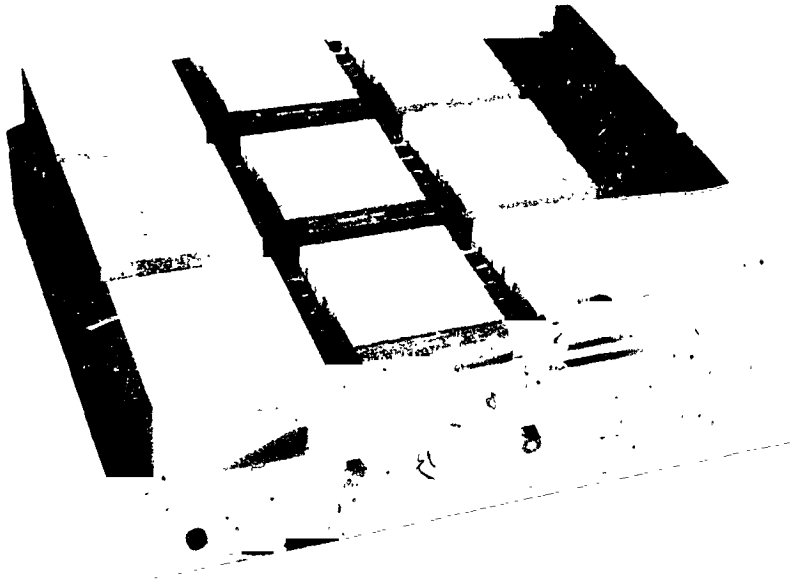
## FINAL STUDY REPORT

### Volume II

N66-21004

FACILITY FORM 802

(ACCESSION NUMBER)	(THRU)
235	1
(PAGES)	(CODE)
CR 65254	08
(NASA CR OR TMX OR AD NUMBER)	(CATEGORY)



GPO PRICE \$ \_\_\_\_\_

CFSTI PRICE(S) \$ \_\_\_\_\_

Hard copy (HC) 6.00

Microfiche (MF) 1.25

**LIBRARY COPY**

JAN 17 1965

MANNED SPACECRAFT CENTER  
HOUSTON, TEXAS

# 853 July 65

**IBM** Federal Systems Division,  
Electronics Systems Center, Owego, New York

AES-EPO STUDY PROGRAM  
Final Study Report  
Volume II

ORIGINATED: \_\_\_\_\_ AES-EPO Staff \_\_\_\_\_

CLASSIFICATION AND  
CONTENTS APPROVAL: JB Lewis

PROJECT OFFICE APPROVAL: Joseph A. Duffley

IBM NUMBER: \_\_\_\_\_ 65-562-012 \_\_\_\_\_

CONTRACT NUMBER: \_\_\_\_\_ NAS 9-4570 \_\_\_\_\_

Prepared for the  
MANNED SPACECRAFT CENTER  
National Aeronautics and Space Administration  
Houston, Texas

**IBM** Electronics Systems Center, Owego, New York

31 December 1965

## FOREWORD

A computer concepts study was conducted at the IBM Electronic Systems Center at Owego, New York, under IBM contract NAS9-4570, for the Manned Spacecraft Center, Houston, Texas. The objective of the study was to investigate possible solutions to long term and time critical reliability problems as they affect the Apollo Command Module guidance and control computer in its application to the AES mission. Volume I of this final report presents a summary of the work performed during the study, and Volume II presents detailed technical descriptions of the various investigations.

## TABLE OF CONTENTS

Section		Page
1.0	PACKAGING . . . . .	1
1.1	Limiting Exposure . . . . .	1
1.2	Connector Sealing . . . . .	8
1.3	Contact Considerations . . . . .	14
1.4	Replaceability . . . . .	23
1.5	Module Size . . . . .	24
2.0	MACHINE ORGANIZATION . . . . .	35
2.1	TMR Characteristics . . . . .	35
2.2	Trade-off Criteria . . . . .	41
2.3	Basic Subsystem Configuration . . . . .	43
2.4	Oscillator . . . . .	63
2.5	Memory . . . . .	70
2.6	Power Supplies and Distribution . . . . .	80
2.7	Grounding . . . . .	86
2.8	TMR/Simplex Mode . . . . .	95
2.9	Reorganized Subsystem . . . . .	99
2.10	Transient Protection . . . . .	125
3.0	ERROR DETECTION AND DIAGNOSIS . . . . .	135
3.1	Approach . . . . .	135
3.2	Disagreement Detectors . . . . .	140
3.3	Switching . . . . .	150
3.4	Crew Requirements . . . . .	156
3.5	Programming Requirements . . . . .	156
4.0	FABRICATION AND TEST . . . . .	166
4.1	Equipment Mockup . . . . .	166
4.2	Exploratory Tests . . . . .	167
4.3	Environmental Simulation Equipment . . . . .	172
4.4	Evaluation Tests . . . . .	176
4.5	Test Results . . . . .	177

## LIST OF ILLUSTRATIONS

Figure		Page
1	Unit Packaging Approach . . . . .	3
2	Computer Casting . . . . .	4
3	Channel Packaging Approach . . . . .	5
4	Cell Packaging Approach . . . . .	6
5	Initial Leakage Rate . . . . .	7
6	Seal Deterioration with Use . . . . .	9
7	Connector Sealing Technique (Modified Saturn - V Connector) . . . . .	11
8	Phase I Test Model . . . . .	12
9	Change in Contact Resistance Versus Time (Gold and Gold Alloy) . . . . .	17
10	Porosity Versus Thickness for Gold Plating . . . . .	18
11	Constriction Resistance Versus Load . . . . .	21
12	Contact Resistance Versus Alloy Gold Content . . . . .	22
13	Interconnections per Circuit Versus Circuits per Page . .	25
14	Connections Versus Logic Blocks . . . . .	27
15	Interconnections per Circuit Versus Circuits per Page . .	28
16	Voters per Page Versus Circuits per Page . . . . .	30
17	Circuits per Machine Versus Circuits per Page . . . . .	31
18	Channel Packaging . . . . .	32
19	TMR Voting. . . . .	36
20	TMR Versus Simplex Reliability . . . . .	38
21	Channel Switching . . . . .	40
22	Module Switching . . . . .	41
23	Saturn-V Voter . . . . .	42
24	Saturn-V Guidance Computer . . . . .	44
25	Data Adapter Block Diagram . . . . .	53
26	Oscillator Synchronization . . . . .	66
27	Transient Filter . . . . .	67
28	Clock Generator . . . . .	68
29	Biased Oscillators . . . . .	69
30	Gated Oscillators . . . . .	71
31	Duplex Memory . . . . .	72
32	TMR Memory . . . . .	73
33	Triplex-Duplex Power System . . . . .	82
34	Interrelated Power System . . . . .	84
35	Grounding System . . . . .	87

# LIST OF ILLUSTRATIONS (Continued)

Figure		Page
36	Regulated DC Return Ground Planes . . . . .	88
37	Module Ground Planes . . . . .	90
38	Discrete Input Circuit . . . . .	91
39	Discrete Output Circuit . . . . .	93
40	Pulse Input Circuit . . . . .	94
41	Pulse Output Circuit . . . . .	94
42	Generalized Reliability Curves . . . . .	96
43	Reliability Comparison (TMR and TMR/Simplex) . . . . .	100
44	Four-Module Partitioning of the Saturn-V Computer . . . . .	102
45	AES Computer Flow Diagram . . . . .	105
46	AES Data Adapter Flow Diagram . . . . .	107
47	AES Computer Subsystem Package . . . . .	110
48	Voting and Disagreement Detection . . . . .	136
49	Module Switching . . . . .	137
50	Saturn-V System Simulator Flow Diagram . . . . .	139
51	Methods of Error Detection . . . . .	141
52	TMR/Simplex Operation . . . . .	152
53	Logic Voter . . . . .	155
54	Detection Distribution in a Diagnostic Program . . . . .	161
55	Apollo Computer - AES . . . . .	168
56	Completed Mockup . . . . .	A-2
57	Representative Module for Phase II Testing . . . . .	169
58	Phase I Test Model . . . . .	171
59	Environmental Test Chamber . . . . .	A-3
60	Functional Diagram-Test Chamber . . . . .	173
61	Chamber During Test . . . . .	A-4
62	Test Fixture . . . . .	A-5
63	Phase II Module Failures (>25 Millivolts)- Module No. 211 . . . . .	180
64	Phase II Module Failures (>25 Millivolts)- Module No. 212 . . . . .	180
65	Phase II Module Failures (>25 Millivolts)- Module No. 213 . . . . .	181
66	Phase II Module Failures (>25 Millivolts)- Module No. 214 . . . . .	181
67	Phase II Module Failures (>25 Millivolts)- Module No. 215 . . . . .	182
68	Phase II Module Failures (>25 Millivolts)- Module No. 216 . . . . .	182
69	Phase II Module Failures (>25 Millivolts)- Module No. 230 . . . . .	183

# LIST OF ILLUSTRATIONS (Continued)

Figure		Page
70	Phase II Module Failures (>25 Millivolts)- Module No. 231 . . . . .	183
71	Phase II Module Failures (>25 Millivolts)- Module No. 232 . . . . .	184
72	Summary of Failures . . . . .	185
73	Nine Modules Under Test - 9 Days . . . . .	A-7
74	Nine Modules Under Test - 27 Days . . . . .	A-8
75	Seven Modules - 27 Days . . . . .	A-9
76	Individual Module - 32 Days . . . . .	A-10
77	Individual Module - 32 Days . . . . .	A-11
78	Individual Module - 32 Days . . . . .	A-12
79	Individual Module - 32 Days . . . . .	A-13
80	Individual Module - 32 Days . . . . .	A-14
81	Individual Module - 32 Days . . . . .	A-15
82	Individual Module - 32 Days . . . . .	A-16
83	Individual Module - 32 Days . . . . .	A-17
84	Module 212 - 32 Days . . . . .	A-18
85	Module 212 Enlargement - 32 Days . . . . .	A-19
86	Module 212 Female Connector - 32 Days . . . . .	A-20
87	Module Pin Discoloration - 32 Days . . . . .	A-21
88	Individual Module - 57 Days . . . . .	A-22
89	Individual Module - 57 Days . . . . .	A-23
90	Individual Module - 57 Days . . . . .	A-24
91	Individual Module - 57 Days . . . . .	A-25
92	Individual Module - 57 Days . . . . .	A-26
93	Individual Module - 57 Days . . . . .	A-27
94	Individual Module - 57 Days . . . . .	A-28

## LIST OF TABLES

Table		Page
1	Physical Comparisons of Packaging Approaches . . . . .	10
2	Contact Resistance (Average of Several Field Sites) . . . . .	15
3	Reliability States for TMR Modules . . . . .	37
4	TMR Computer Characteristics . . . . .	50
5	Data Adapter Characteristics . . . . .	52
6	Address Groups . . . . .	52
7	Reliability Estimates (Basic System) . . . . .	64
8	Regulated DC Power per Section . . . . .	83
9	Power System Component Count . . . . .	85
10	Computer Sizing . . . . .	101
11	TMR Computer Characteristics (AES) . . . . .	106
12	Data Adapter Modules . . . . .	109
13	Reliability Estimates (AES System - TMR Mode) . . . . .	115
14	Reliability Estimates (AES System - TMR/Simplex Mode) . . . . .	115
15	List of Available Spares . . . . .	117
16	On-board Spares - 100-Percent Duty Cycle . . . . .	118
17	On-board Spares - 50-Percent Duty Cycle, Non-op Failure Rate > 0 . . . . .	118
18	On-board Spares - 25-Percent Duty Cycle, Non-op Failure Rate > 0 . . . . .	119
19	On-board Spares - 50-Percent Duty Cycle, Non-op Failure Rate = 0 . . . . .	119
20	On-board Spares - 25-Percent Duty Cycle, Non-op Failure Rate = 0 . . . . .	120
21	Reliability Improvement Due to Sparing . . . . .	120
22	AES System Reliability - Re-entry Phase . . . . .	121
23	AES System Mission Reliability . . . . .	121
24	AES System Reliability - Switchable Spare Mode . . . . .	122
25	AES System Reliability - Total Mission . . . . .	122
26	Disagreement Patterns . . . . .	125
27	Diagnostic Listings . . . . .	126
28	Signals, Logic, and Voters . . . . .	144
29	Additional Disagreement Detectors . . . . .	145
30	Distribution of Detectors . . . . .	145
31	Error Signal Propagation . . . . .	147
32	Typical Print-out from Redundant Computer Simulation . . . . .	149
33	Typical Redundant Computer Simulation . . . . .	150
34	Symptom - Failure Correlation . . . . .	162
35	Computer Symptoms . . . . .	163
36	Test Equipment Listing . . . . .	174
37	Test Schedule . . . . .	177

## 1.0 PACKAGING

The packaging scheme of the Saturn V computer and Apollo back-up data adapter was examined to determine its applicability to inflight maintenance, sparing, and module and channel switching in the high humidity - zero gravity AES environment. Consideration was then given to other packaging techniques which would improve operation in this environment without resorting to hermetic sealing. Techniques that required maintenance tools which could not be used by a suited astronaut were not considered in this study.

The study approach to the packaging problem was to first examine methods for sealing the replaceable modules within the computer and data adapter frame to provide gross protection against the high humidity-zero gravity environment and then to examine methods for providing additional environmental protection on the replaceable module level, especially at the connectors. Since any sealing method is imperfect, especially over long periods of time, a study was made of available contact materials and connection techniques to ensure proper operation of the module and cable connectors in the presence of the contaminants which manage to penetrate the equipment sealing features. Finally, consideration was given to size and connection constraints on the replaceable module which would affect the physical organization of the computer and data adapter.

### 1.1 Limiting Exposure

A repackaging study was performed to determine the feasibility of sealing the computer and data adapter circuits for operation and maintenance in the high humidity-zero gravity AES environment. The approach investigated to provide operation in the adverse environment was gasket sealing with a slight overpressurization of the units maintained by periodic repressurization. Maintenance of the circuits would be allowed by resealing, purging, and repressurization after repair.

Almost perfect purging of gasses and water vapor and very short purging time periods are feasible by venting the sealed equipment to space. The installation of heaters within the computer and data adapter to operate during periods when a cover is removed and during purging would provide additional assurance against the accumulation of contaminant gasses and vapors. The circulation of hot fluid through the coolant system of the unit being purged or repaired would provide protection equivalent to heaters, as would the application of external infrared heaters or dry air blowers.

Treatment of the internal surfaces of the computer (including electrical connections) with hydrophobic film would tend to prevent the condensation of moisture on critical areas, and where moisture did condense it would tend to form into droplets instead of thin films. The entire interior of the computer could be treated with any of several available silicone sprays on assembly, and solid silicone compounds could be applied during maintenance in the zero gravity environment where sprays would be impractical.

Closed loop pressure systems were considered but will not be emphasized in the study. The use of freon in a closed loop system (or even in a static system) offers several advantages including moisture repellent characteristics.

Three approaches to packaging the computer for operation and maintenance in the AES environment were examined and compared. These three approaches differ in the level of packaging to which the sealing and purging techniques are applied. Although the preliminary investigations were related only to the computer, the concepts apply as well to the data adapter.

In the first approach the entire computer is sealed as a unit as shown in Figure 1. Upon removing one of its two covers to replace a failed module, the entire computer is exposed to the adverse AES environment. When the cover is replaced after repair, the free moisture and contaminants trapped in the computer are purged and the computer repressurized to somewhat greater than cabin pressure with dry gas.

In the second and third approaches an attempt is made to limit the degree of exposure during a maintenance action by sealing various portions of the computer independently. Since a triple modular redundant (TMR) computer consists of essentially three individual computers, each channel can be separately sealed so that one third or less of the computer is exposed each time a repair is attempted. The casting of the Saturn V computer is designed such that each logic channel is partitioned into effectively five cells as shown in Figure 2. If each cell is separately sealed, then a fifteenth or less of the computer is exposed each time a repair is attempted. These second and third packaging approaches are illustrated in Figures 3 and 4, respectively.

The computer covers can be sealed by means of special gaskets or modified O-rings. Gasket-sealed electronic units have been produced at IBM to provide leakage rates as low as  $10^{-7}$  cubic centimeters per second per inch of linear seal length for ASQ-38, Gemini, and other applications. The larger covers, especially those of the first approach above, would preclude leakage rates as low as this so that periodic

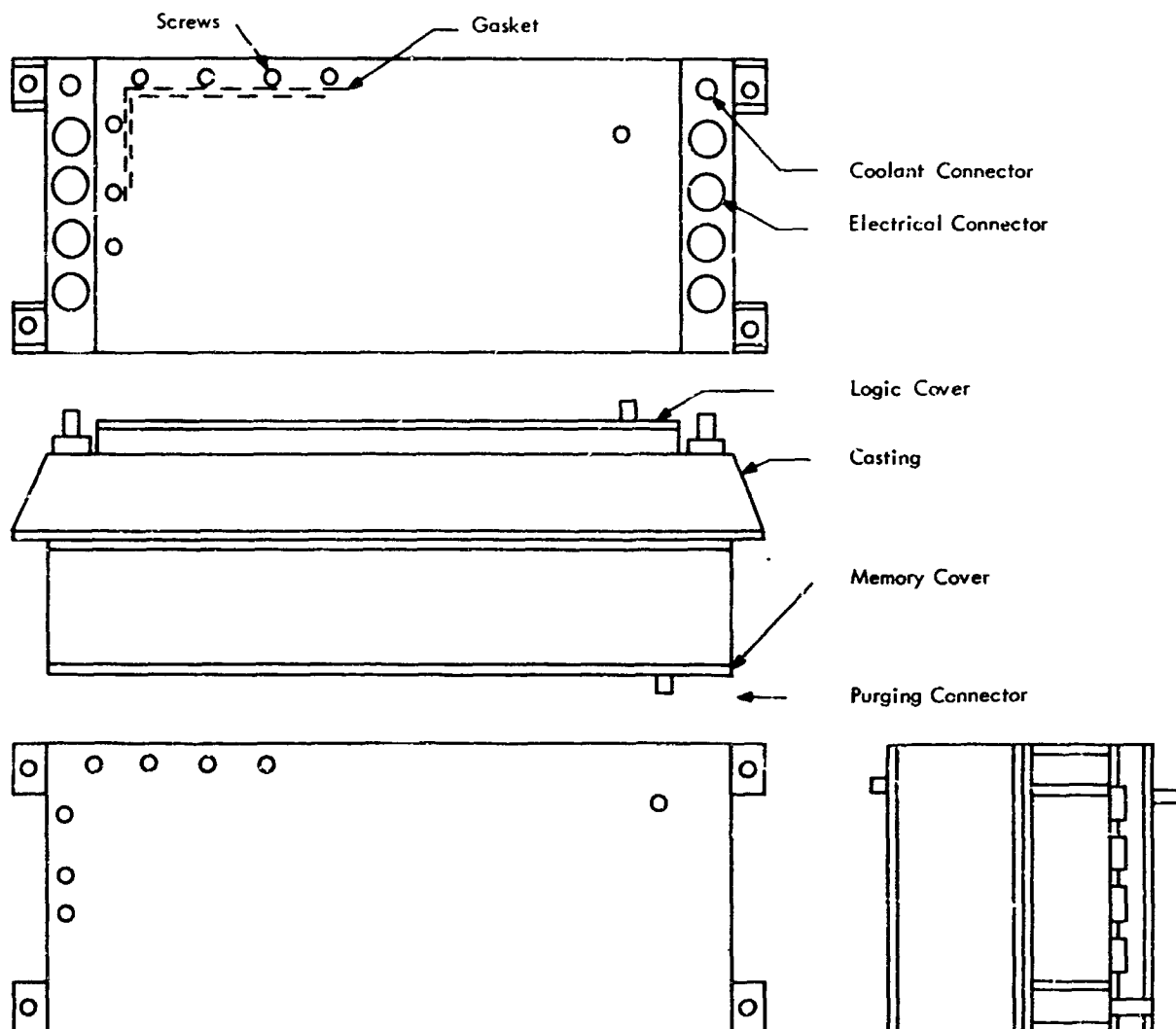


Figure 1. Unit Packaging Approach

repressurization of the computer and data adapter would be required. Figure 5 shows how the residual gas pressure of the proposed designs would decrease with mission time.

An examination of Figure 5 reveals the following information:

- 1) The unit-seal approach affords the lowest leak rate (because its linear seal length to volume ratio is the smallest). For the same reason, the leakage rates from the memory modules are less than the leakage rates from the logic modules for both the cell-seal and channel-seal designs.

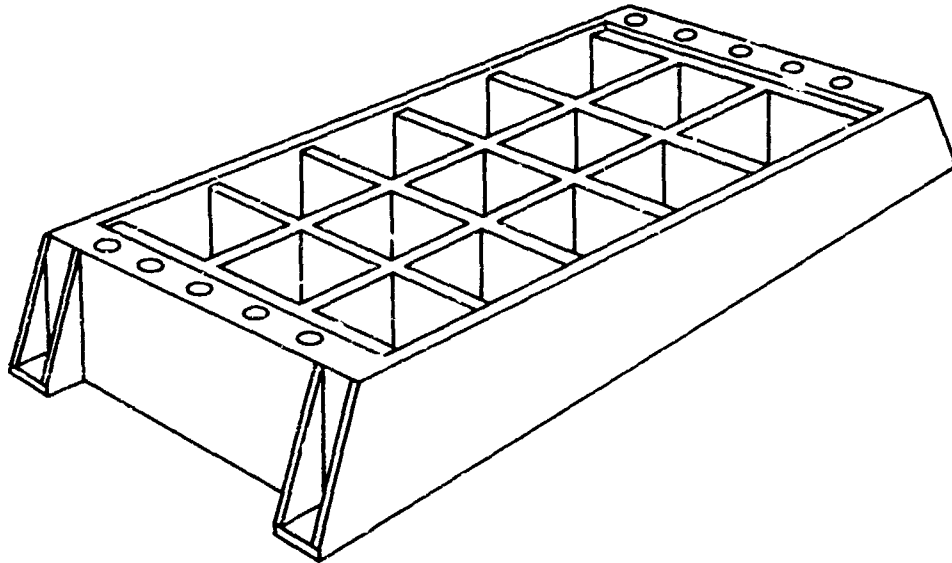


Figure 2. Computer Casting

- 2) If the assumption is made that a module replacement occurs on the average of once a week during the 90-day mission (10 logic failures and 3 memory failures per mission), then the time period for which the seal is effective (defined as the period during which the residual pressure exceeds 50 percent of the initial overpressure) is determined by the component failure rate of the computer rather than by the leakage rates for both the unit-seal and channel-seal designs. These factors are tabulated from Figure 5 as follows:

Sealing Level	Time Period (days) to	
	Failure	50% Pressure
Unit Logic	4 1/2	90
Unit Memory	15	90
Channel Logic	15	25
Channel Memory	45	90

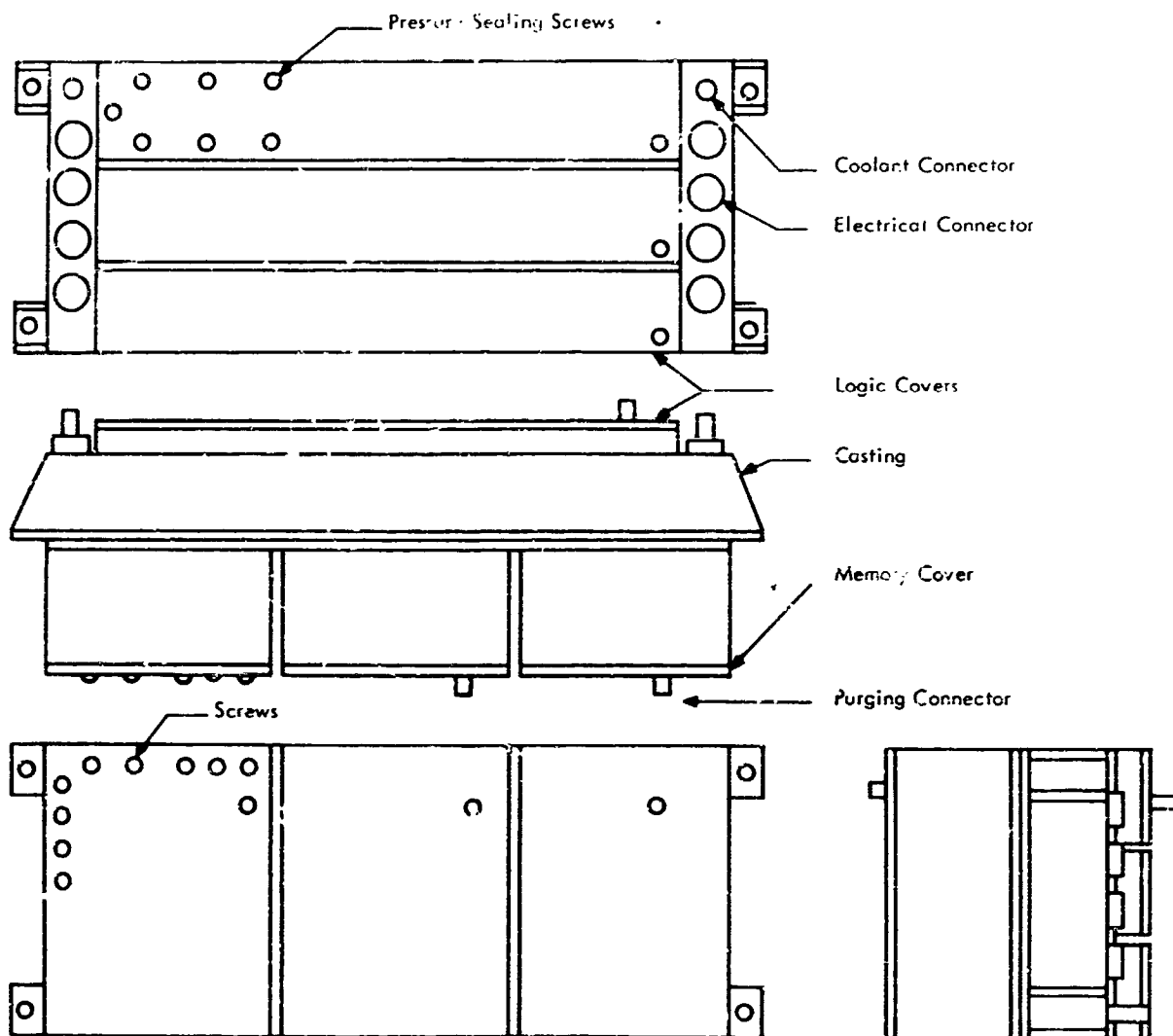


Figure 3. Channel Packaging Approach

- 3) For the same assumptions, the time period for which the seal is effective for the cell-seal design is determined by leakage rate rather than component failure rate. The following values were taken from Figure 5.

Sealing Level	Time Period (days) to	
	Failure	50% Pressure
Cell Logic	67	16
Cell Memory	90	55

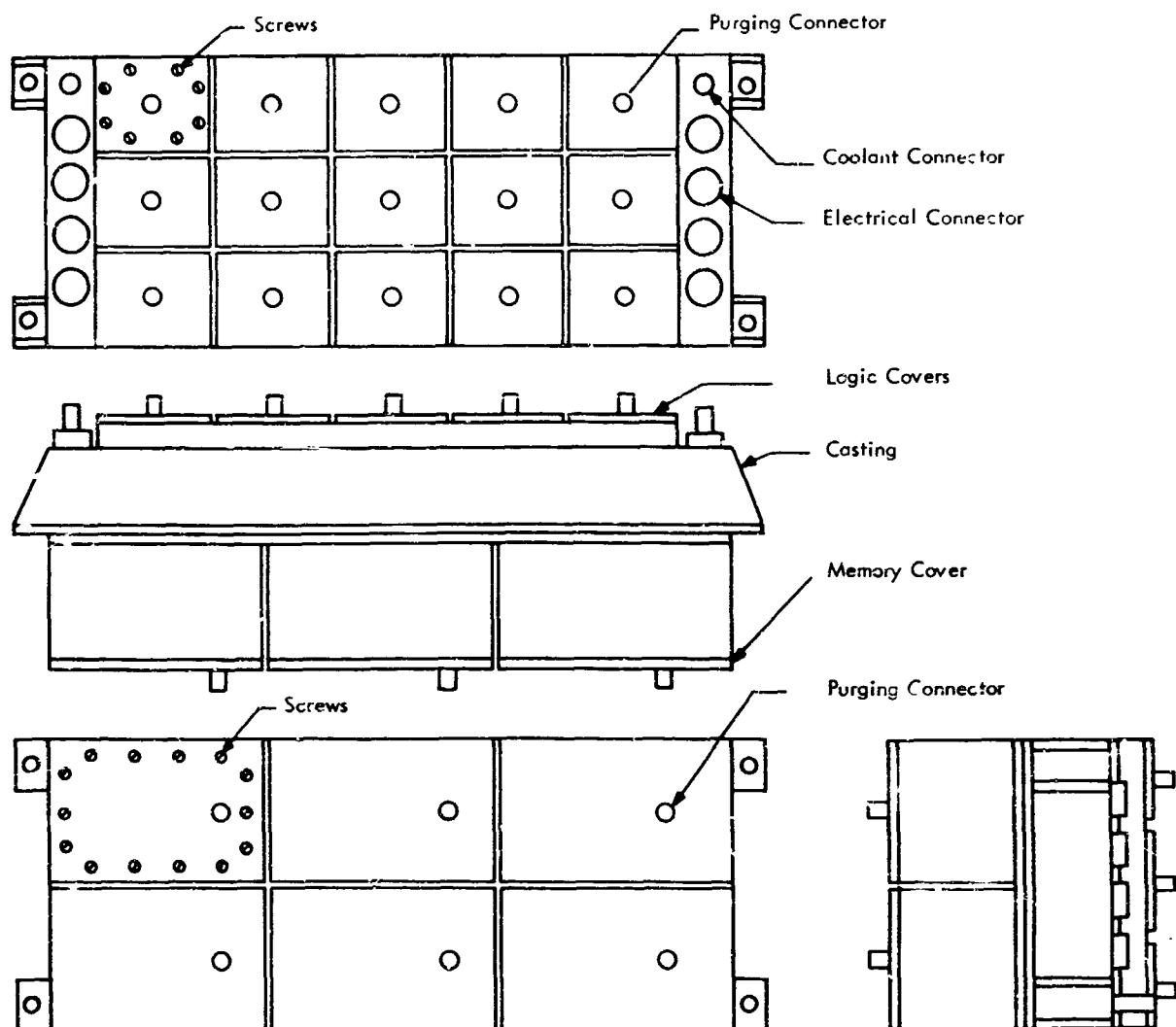


Figure 4. Cell Packaging Approach

No attempt was made in the leakage rate computations to account for the probable differences in efficiency of the various sealing approaches. Experience at IBM has indicated that the leakage rate of a large seal (such as an entire computer cover) compared to that of a small seal (such as an individual cell cover) is greater than that predicted simply by a difference in the linear length of the seal. This effect is due to the greater difficulty in maintaining tolerances, parallel sealing surfaces, and uniform sealing pressure with larger units. If this effect were taken into account, the curves of differential pressure versus mission time would be grouped closer together.

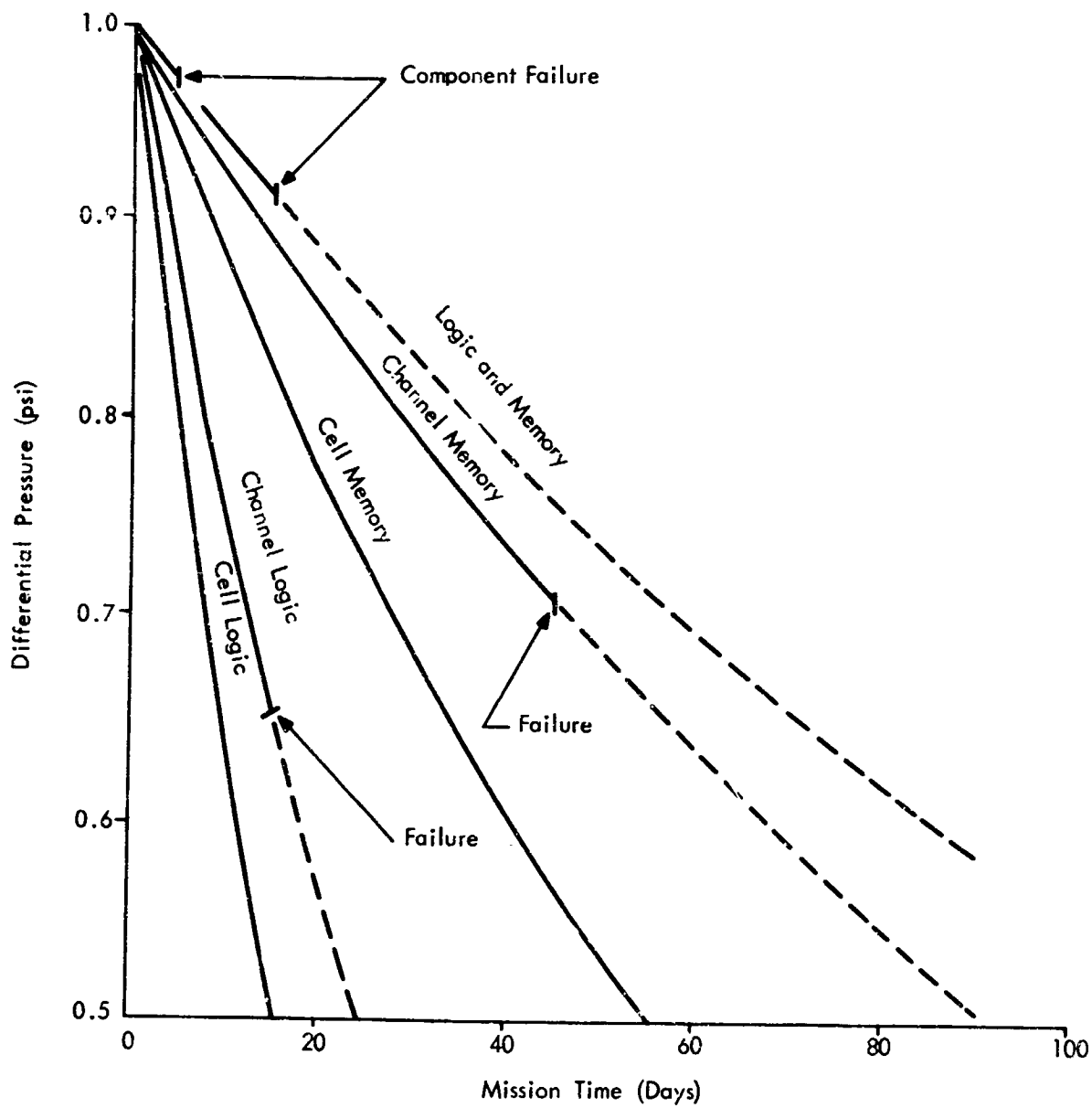


Figure 5. Initial Leakage Rate

In addition, other maintenance features favor the cell-seal design. An average of about 9 screws would have to be removed every time a failed module is replaced in the cell-seal design compared to 23 screws for the channel-seal and 32 screws for the unit-seal designs. The exposed volume per repair is about as follows:

Cover Removed	Volume Exposed (in <sup>3</sup> )		
	Unit	Channel	Cell
Logic	1500	125	25
Memory	1500	300	150

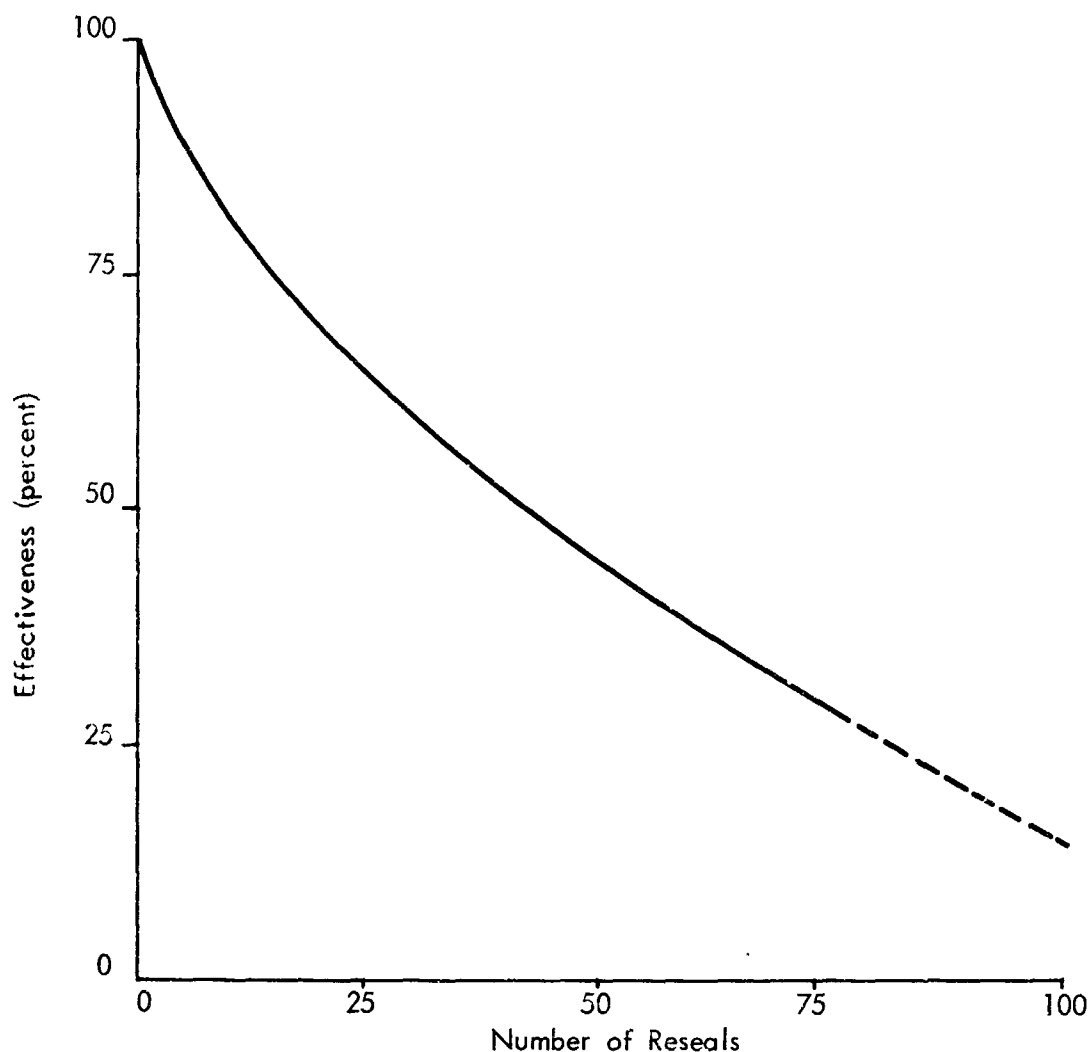
Gasket seals have a tendency to deteriorate with usage. Each time a seal is broken and then resealed, the effectiveness of the seal is compromised. Figure 6 is an estimate, based on IBM experience, of the effectiveness of a gasket seal versus use in the AES mission.

Repackaging the computer into independently sealed cells provides an improvement in ease of maintenance and in exposure to the AES environment during repair. The average number of screws which must be removed to replace a failed module is less than a third and a half, respectively, of that of unit and channel sealing, respectively. The amount of circuitry exposed during a repair is less than a twentieth that of unit sealing and a fifth that of channel sealing.

The advantages of cell sealing over the other two approaches are obtained at the cost of somewhat increased size and weight, as indicated in Table 1. Since the advantages appear to outweigh the disadvantages, the cell or honeycomb approach would be recommended over the other two approaches.

## 1.2 Connector Sealing

Even if fairly efficient protection of the replaceable modules is achieved by sealing the modules within the computer and data adapter frame and by limiting the exposure of the modules to the high humidity-zero gravity environment, some free moisture and contaminants will collect eventually at the module connectors. Whatever packaging techniques are selected for AES applications, the problem of sealing the intermodule and inter equipment connectors against the high humidity-zero gravity environment will exist.



**Figure 6. Seal Deterioration with Use**

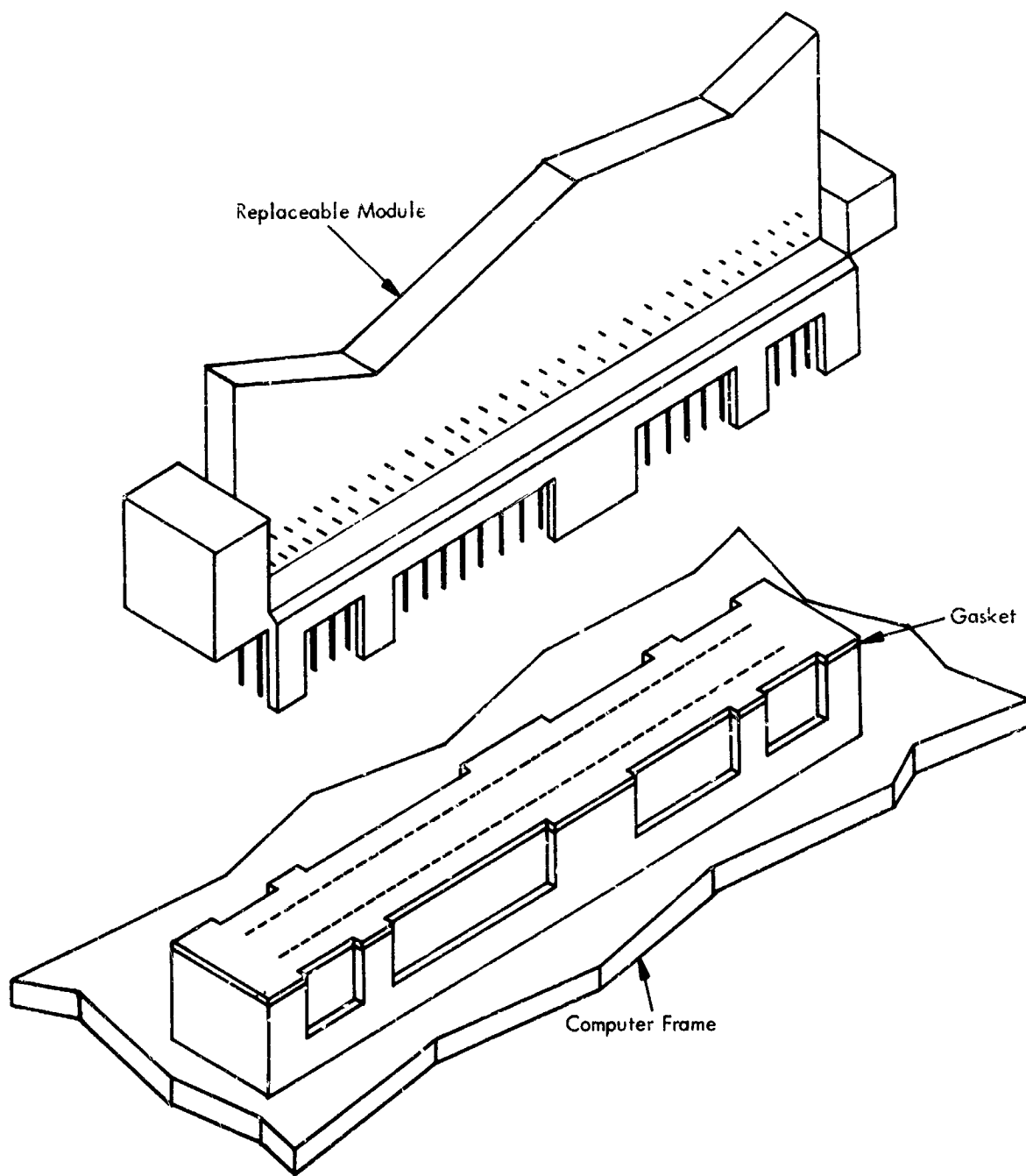
Design analysis and exploratory testing of methods of sealing the connector of a replaceable module resulted in the selection of a gasket-silicone gel technique for the representative module to be demonstrated according to the study test plan. As shown in Figure 7, a silicone rubber gasket was cemented to the face of the female connector. The female connector was then loaded with a silicone gel. The male pins on the replaceable module were also coated with silicone. Since the slotted holes in the gasket are somewhat smaller than the male pins, a wiping action occurs both on insertion and on removal of the replaceable module. This wiping action serves to remove moisture from the male pins on insertion and to retain the silicone gel in the female receptacle upon removal of the replaceable module. This concept was used in the Phase II Testing.

TABLE 1 — Physical Comparisons of Packaging Approaches

Physical Characteristics	Deviation from Saturn V (percent)		
	Unit	Channel	Cell
Volume and Mounting Area	+ 6	+ 13	+ 17
Weight	+ 1	+ 3	+ 5
Screws/Maintenance Action	Ref.	- 25	- 75
Exposed Volume/Maintenance	Ref.	- 65	- 90
Leakage Rate --- Initial	Ref.	+ 75	- 25
--- End of Mission	Ref.	+ 30	- 80

Phase I testing included investigations of gasket seals on the interface between the male and female connectors, sealing of the connectors with various greases, and combinations of gaskets and greases. The technique showing the most promise is sketched in Figure 8. A male and female Saturn-V page connector were wired and sealed with epoxy on their rear surfaces. A silicone rubber gasket was glued to the face of the female connector with Dow-Corning A9-4000. The female cap was removed and DC-3 silicone grease packed inside the connector. The pins of the male connector were also saturated with DC-3 silicone grease. Contact measurements before and after application of silicone grease indicated that the grease had no measurable effects on the contact resistance between male and female connections. Leakage resistance checks between adjacent pins were made under the following conditions:

- 1) Initial leakage resistance of mated test model — 500,000 megohms;
- 2) Immersed mated connector in fresh water for 15 seconds and shook off excess water — 2,000 to 10,000 megohms, erratic



**Figure 7. Connective Sealing Technique (Modified Saturn-V Connector)**

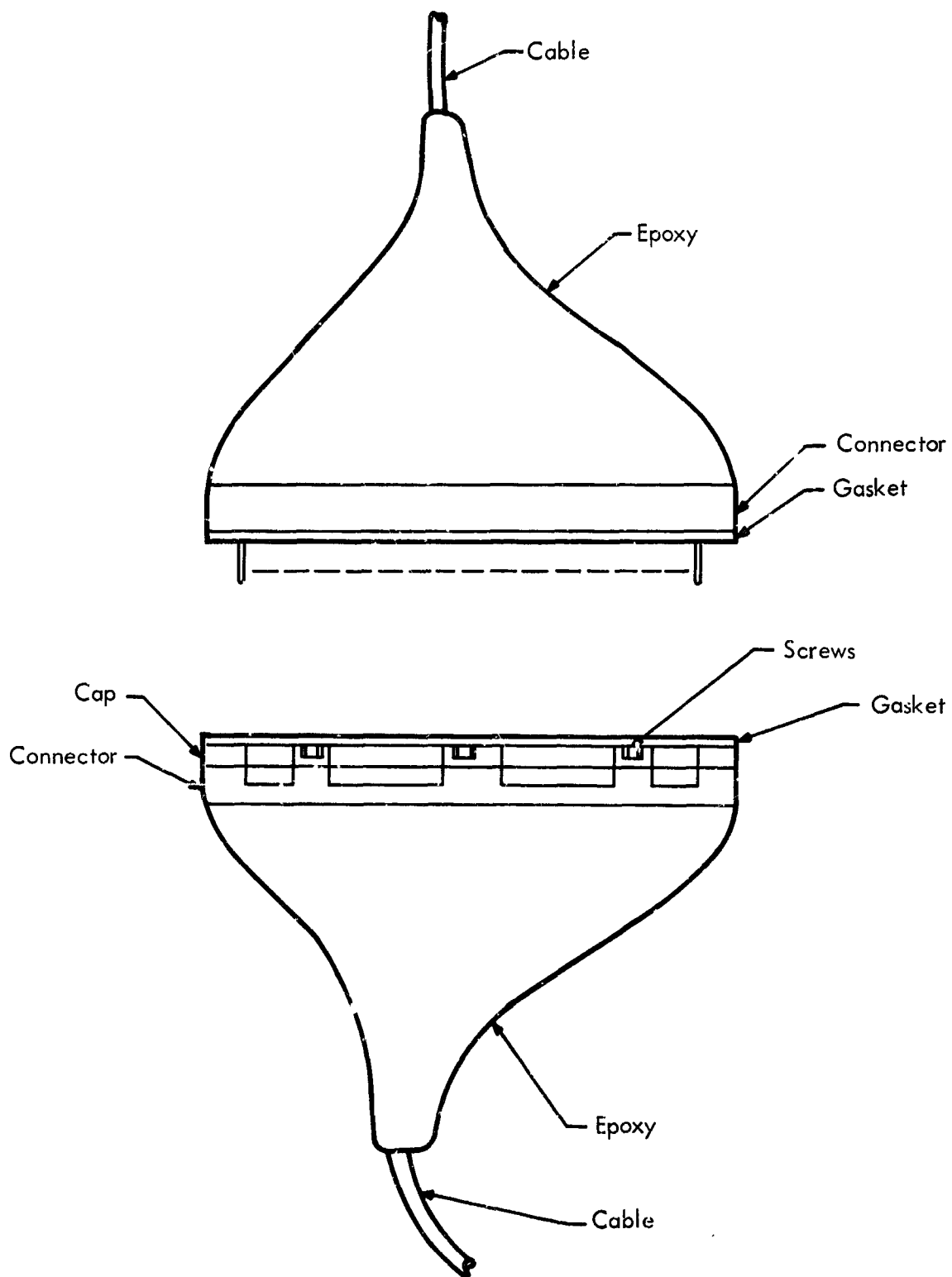


Figure 8. Phase I Test Model

- 3) Unmated connector, dried male for 20 seconds at 125 degrees Fahrenheit, remated — 140,000 megohms
- 4) Unmated connector, immersed both halves in fresh water for 15 seconds, shook off excess water, remated — 70,000 megohms
- 5) Unmated connector and remated — 5,000 megohms
- 6) Unmated connector and remated — 70,000 megohms
- 7) Unmated connector and remated — 85,000 megohms
- 8) Unmated connector and remated — 60,000 megohms
- 9) Unmated and remated connector under fresh water — reading erratic;
- 10) Unmated connector and shocked water off male connector on desk top, remated — 50,000 megohms
- 11) Unmated connector and remated — 10,000 megohms.

Although the preceding readings appeared erratic, they were very encouraging from the following viewpoints:

- 1) The lowest leakage resistances were still in the thousands of megohms
- 2) The surface between the cap and connector of the female and the screw holes in the female presented sources for leakage which were sealed during Phase II tests.
- 3) The large holes in the female gasket which allow penetration of the male pins also allowed penetration of excess moisture.

The same test was essentially repeated in a salt water solution with no significant changes.

Another material used to seal the female connector was Dow Corning Sylgard 51 dielectric gel. When cured, it develops into a soft, transparent, jelly-like mass having good self-healing qualities. Different consistencies were used, but none were found to be satisfactory. All had a tendency to be drawn out when the connector was unmated.

The most optimum sealing would be achieved by sealing the female connector with a gasket without the need of impregnating with silicone gels. A most promising concept is that of a membrane which has qualities of self-sealing when unmated. Special tools would be required to fabricate this type of gasket.

Under any conditions, a new development program would have to be initiated for a connector for this application. The new connector would be a molded one-piece connector with a self-contained gasket containing approximately 200 self-sealing holes.

### 1.3 Contact Considerations

An investigation was performed to determine the best contact material for use in the AES connector application. Work performed in IBM's field test program was included in this investigation.

The data of Table 2 presents partial results of a continuing IBM environmental field test program to determine certain properties of electrical contact materials. The tests were performed for a period of over a year at several test sites representative of a variety of environmental conditions. Relative humidity at these sites varied from around 10 to over 80 percent. Measured airborne contaminants included various amounts of NO<sub>2</sub>, HF, NH<sub>3</sub>, SO<sub>2</sub>, O<sub>3</sub>, CL<sub>2</sub>, and H<sub>2</sub>S. Ambient temperatures varied over a range from 60° to 100° F. Table 2 shows a summary of the original values of contact resistance for the contact materials tested and the values after 1 year of environmental exposure. The values in the table were obtained by averaging the data from several test sites.

Use of copper alloys or other of the high resistance materials listed in Table 2 would not be considered for use as contact material in AES applications. Some of the data showed practically infinite resistance after 1 year of exposure to the most adverse environments. Although not indicated in the table, caution should be exercised in the use of palladium or palladium alloys containing copper where high concentrations of organic materials may be encountered. Because of the catalytic nature of palladium, polymers may form in a high organic atmosphere.

TABLE 2 — Contact Resistance (Average  
of Several Field Sites)

Resistance (ohms)	Original	After 1 Year
100		Aluminum, Nickel-Silver, Beryllium Copper, Cop- per, Phosphor Bronze, Brass, Nickel, Silver- Cadmium Oxide
0.01 to 100	Aluminum, Nickel-Silver, Phosphor Bronze, Brass, Nickel	Red Gold, Green Gold, Silver
0.001 to 0.01	Beryllium Copper, Cop- per, Red Gold, Green Gold	Tin, Tin-Lead, Rhodium, Platinum, Platinum- Iridium
0.001	Silver, Silver-Cadmium Oxide, Tin, Tin-Lead, Rhodium, Platinum, Platinum-Iridium, Gold	Gold

The films that form on the surface of silver tend to be highly resistive, coherent, and tenacious if the major ingredient is silver sulfide. However, if appreciable amounts of silver chloride are present, the film may be nonadherent and of moderately low electrical resistance. Although the average contact resistance after 1 year was indicated in Table 2 as 0.01 to 100 ohms, the measured values at the various sites varied over the range bracket of 0.001 to over 100 ohms. Although silver would be very applicable in controlled environments, it will not be considered further in this study.

Samples of 10, 14, and 18 carat green-gold alloys (simple solid solutions of gold and silver) showed characteristics similar to silver in wide variations of contact resistance with environment. Although the variations were less extreme because the films were thinner in proportion to the gold content, caution should be used in the use of green gold alloys for AES applications. Red gold alloys (solid solutions of gold and copper) compared generally with green gold and the same conclusions apply.

The oxide films of tin, lead, and other soft metals tend to be coherent, self-limiting, and thin. These films are easily penetrated under pressure as the soft-bulk material yields. Despite the apparent attractions of tin, lead, indium etc., their use is not recommended for low-load separable-contact applications, especially in sliding situations where wear debris can build up.

Gold and gold alloys would seem to be best applicable as contact materials for AES connectors. The excellent behavior of gold and gold alloy with exposure time is shown in Figure 9. The higher platinum content alloy (6-percent platinum, 25-percent silver, 69-percent gold) is probably preferred although more test data is required for a firm decision. Visible films do exist on exposed gold surfaces but consist of absorbed material rather than tarnish products. SMS gold and 24-carat gold showed similar properties during the tests.

Since gold and low resistance gold alloys are soft materials, their primary use as contact materials to date has been in the form of gold plating over base materials such as nickel or copper. The major problem in this application has been the porosity of the plating, which leaves the porous areas of the basic materials exposed to contamination. Resulting degradation of the contact surface can occur in two different ways.

When the base material exposed under the pores in the gold plating are attacked by contaminants such as sulfur, chlorine, and nitrous oxide, the resulting sulfides, chlorides, and nitrates will migrate through the gold pores and spread out over the surface of the contact, forming high resistance films. Although these creeping films may be controlled by means of surface lubricants or choice of base material, the primary solution will probably be controlled porosity.

The second phenomenon which porous plating invites is electrolytic activity at the base material in the presence of moisture and active atmospheric contaminants. Flaking of the gold plating itself can result as well as formation of resistant films by the migration of corrosion products to the contact surface.

Both types of contact degradation dictate that the porosity of the gold plating be minimized. The obvious approach is to increase the thickness of the plating. However, Figure 10 shows that although the porosity does decrease as plating thickness increases, the curve levels off at the higher thicknesses. This curve represents an average of data at IBM and elsewhere and is plotted relative to the plating porosity at 50 mils plating thickness as standard (or unity). Because of practical considerations, plating thicknesses over 150 mils are not being considered at IBM.

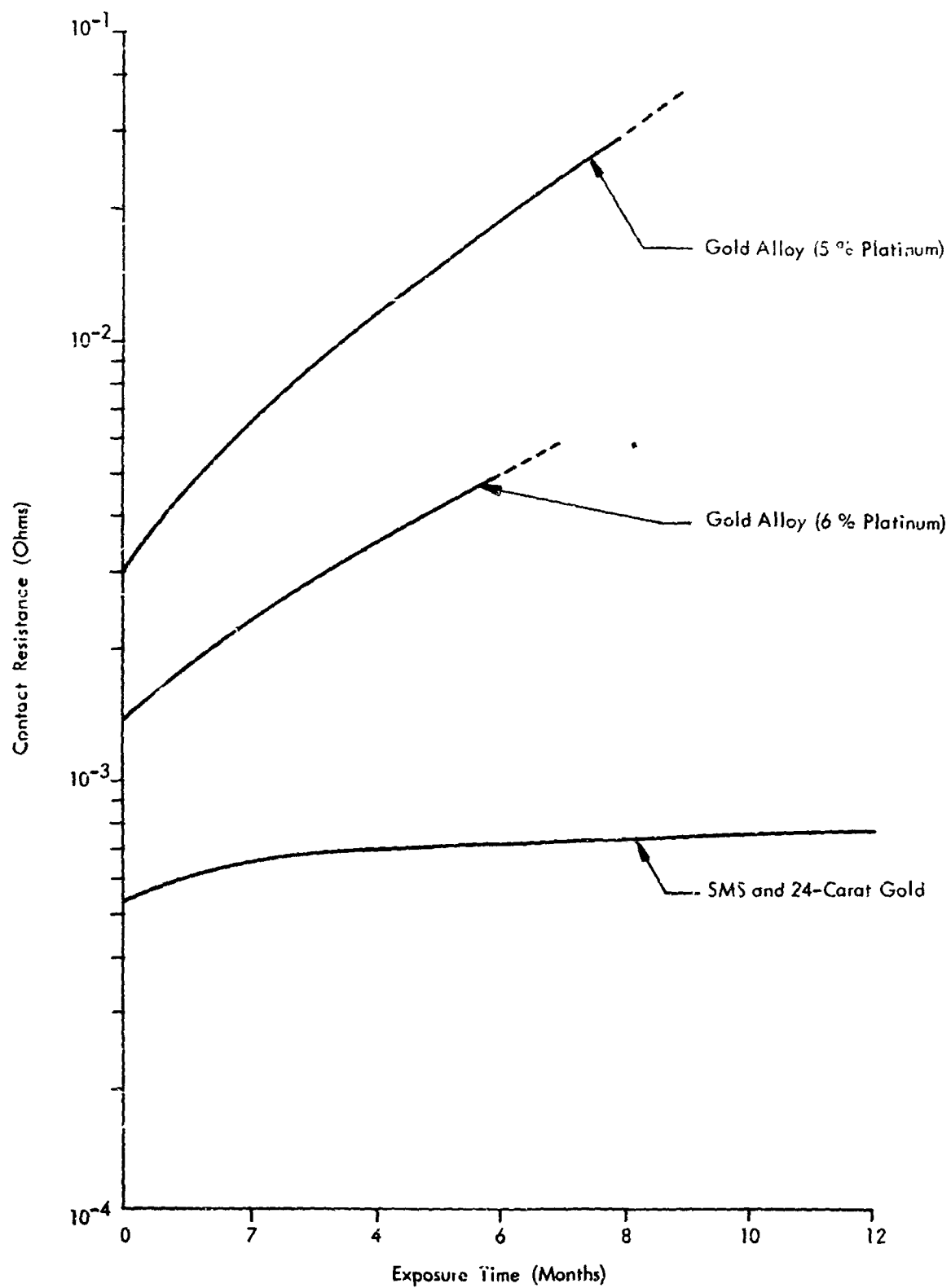


Figure 9. Change in Contact Resistance Versus Time  
(Gold and Gold Alloy)

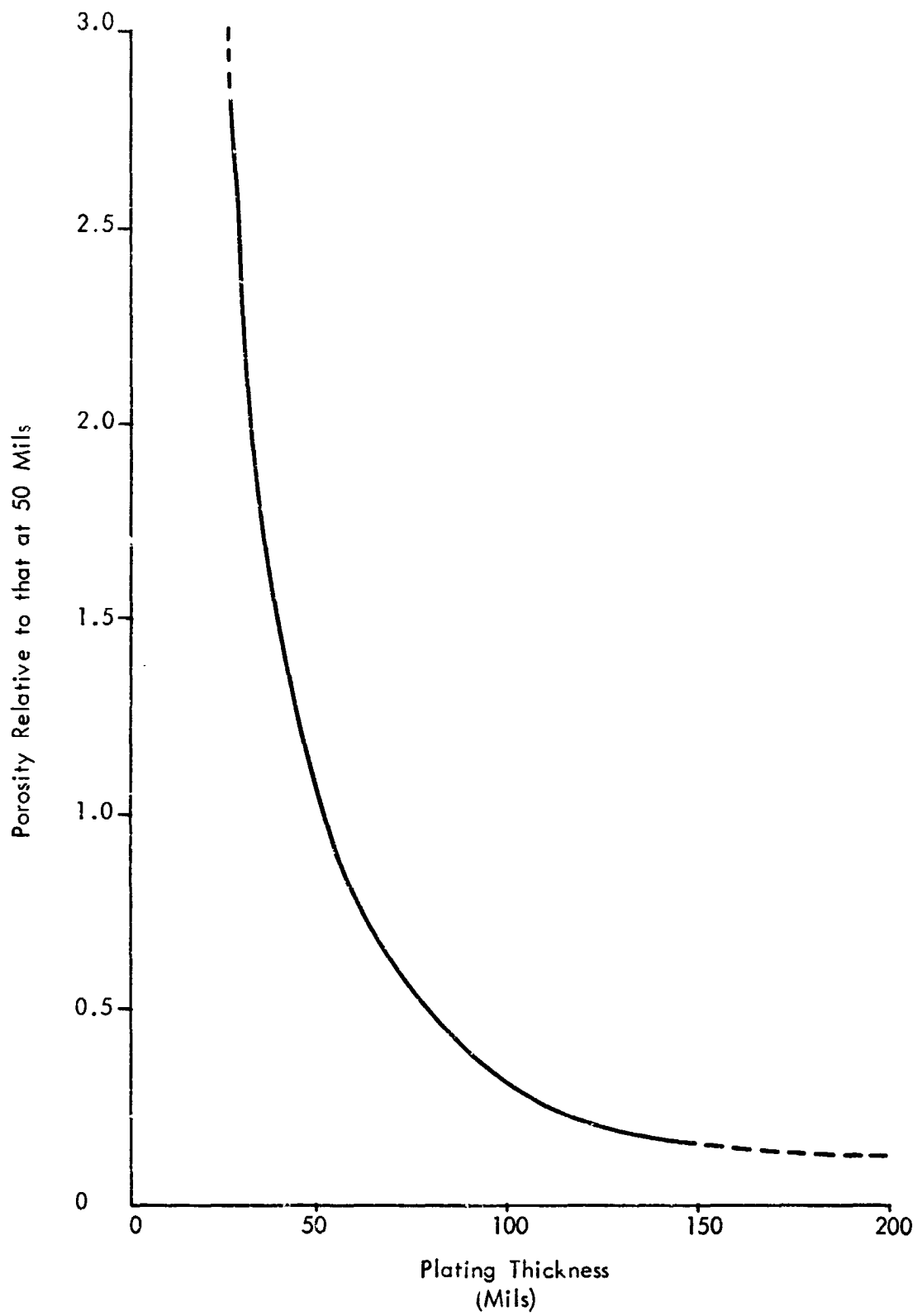


Figure 10. Porosity Versus Thickness for Gold Plating

However, experience has shown that other considerations such as production and testing methods tend to predominate over actual plating thickness in determining porosity at the higher thicknesses. For example, an increase in thickness from 50 to 150 mils was obtained in one case by increasing current density rather than increasing processing time, and the resulting thick plating had higher porosity than the thin plate. The degree to which porosity can be minimized is very sensitive to the cleaning and handling techniques used on the base material.

Porosity of the final product can be controlled by adequate testing of the plating to screen out those samples exceeding a predetermined limit. For critical applications such as AES, the limit can be set much more stringently than the limits set for commercial grade platings. Very sensitive electrographic testing methods are used at IBM in which an electrolyte-saturated filter pad is wrapped around each contact and a small current made to flow from the contact through the pad. After a fixed time period, a reagent applied to the pad indicates the porosity by color test.

Protective contact coatings have been produced by welding gold foil onto the base contact material rather than by plating. Although this method has essentially eliminated the porosity problem associated with plating methods, it has not proven suitable for commercial applications because of the inherent cost of the process and because of the difficulty in producing uniform coating thickness. This technique should not be overlooked, however, for low quantity-highly critical applications such as AES.

Multilayer platings are generally more expensive than single layer platings of the same total thickness and are therefore not favored for high production commercial applications. However, when a contact surface is built up from several layers of gold plating, there will exist some misalignment of the porosity of the individual layers and a resulting decrease in effective porosity over that of a thick coating deposited as a single layer.

Even if the problem of porosity is solved by pursuing those methods which have been rejected for commercial applications because of cost or of the difficulties in mass production, a problem may still exist in the form of diffusion, which in the migration of base contact material or impurities through the plating material itself rather than through the pores. The transferred materials form resistive films on the surface of the gold plating in the same manner as those caused by porosity. Some commercial applications use an intermediate barrier layer of nickel between a base material of copper and the gold plating to retard diffusion. Rhodium was found to exhibit the highest retardation capability as a barrier layer but was considered too expensive, too difficult to process, and too brittle for commercial use.

The choice of plating and base contact materials must also be made after consideration of the possibility of galvanic corrosion. To prevent galvanic action, metals in relatively close position in the electromotive series should be chosen for plating and base materials.

It appears that the choice of nickel as the base material with gold as a thick-film surface material is best suited for AES applications in view of all the preceding considerations. The thick film should be built up by several successive electrodeposits or, preferably, by welding gold foil on the nickel contact pins. Very stringent process and testing methods must be applied, which will surely result in very high rejection rates. Although the resulting connector costs will be considerably higher than the costs of presently employed commercial connectors, the pin corrosion problem would be minimized for the AES applications, and the costs seem to be justified for low quantity, highly critical usages.

The resistance of an electrical contact is made up of two components: 1) constriction resistance due to the convergence of current flow lines to points of contact and 2) film resistance due to impedance of electron flow by the surface films.

Constriction resistance varies primarily with the resistivity of the contact material, the contact load, and the contact geometry. Figure 11 shows the resistance of several contact materials measured with a 1/8-inch diameter, spherically shaped gold probe tip. The curves indicate the manner in which constriction resistance varies with contact load for given contact geometry and material. Note that some of the curves cross, suggesting that the choice of contact material for a given connector design may be made on the basis of the contact load of that connector. However, consideration must first be given to film resistance.

Contact films are the result of reaction of the contact material with one or more contaminants in the environment or absorption of impurities by the contact surface. In general, all metals except pure gold will form reaction films. Gold alloys will form reactant films in proportion to the amount of alloying material as indicated in Figure 12. The curves were derived from IBM field test data. Gold alloys may be required in AES applications to provide sufficient hardness and wear resistance.

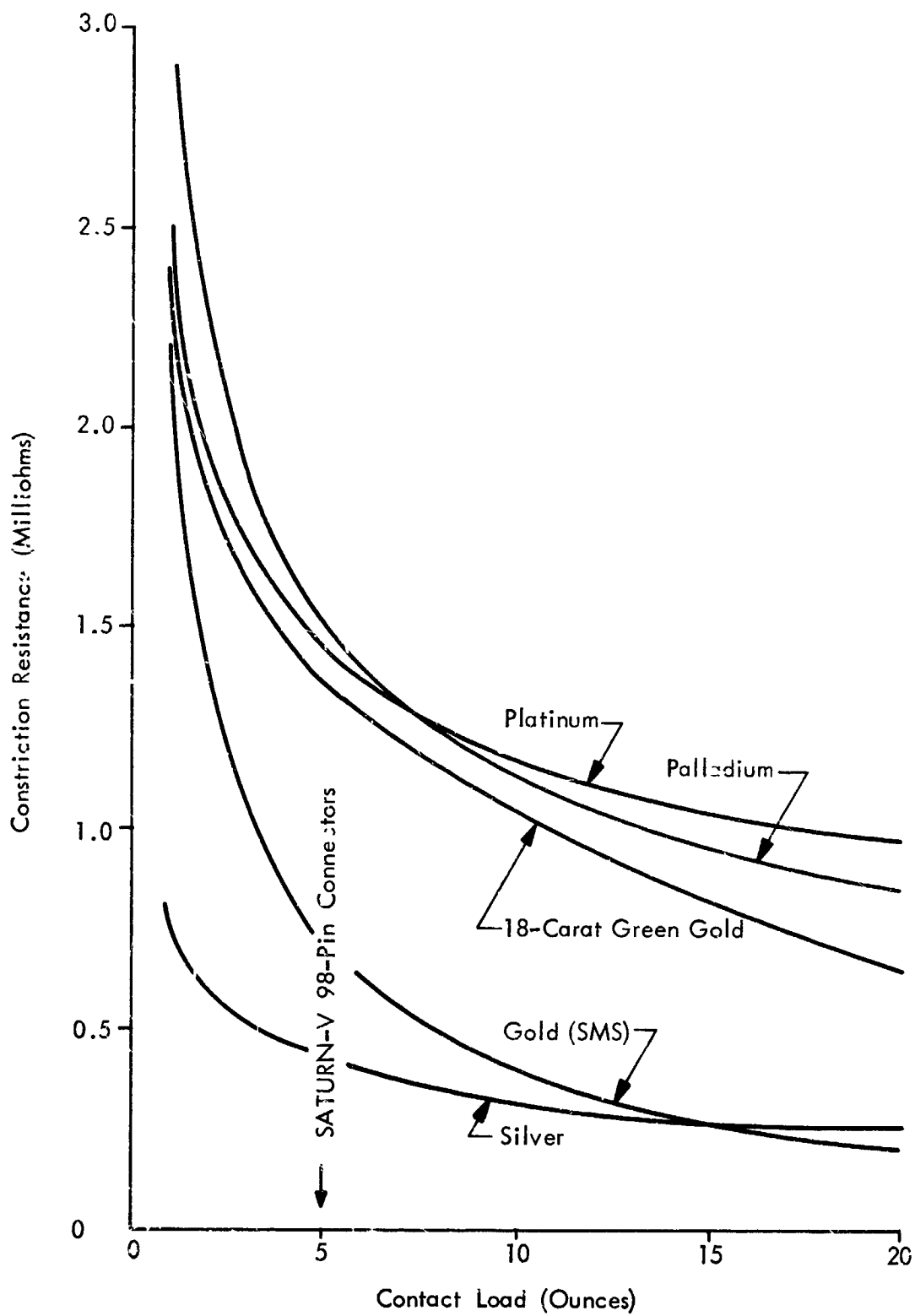


Figure 11. Constriction Resistance Versus Load

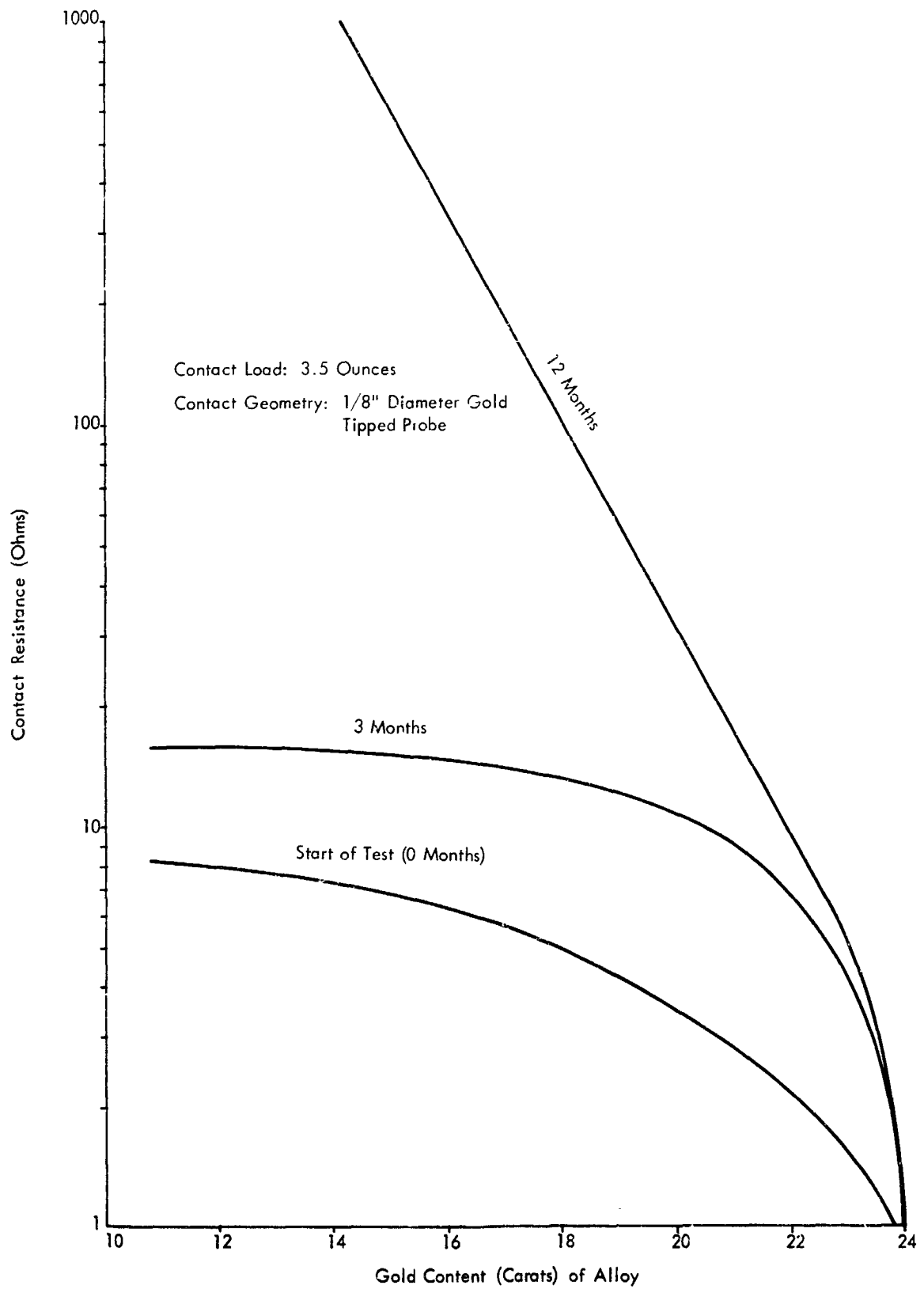


Figure 12. Contact Resistance Versus Alloy Gold Content

#### 1.4 Replaceability

Inflight maintenance, for prolonged missions, requires the careful analysis of certain aspects of packaging and accessibility requirements of man-rated electronic equipment. One of these aspects is replaceability.

Replaceability is defined as the proper restoration or substitution of like modules in a system or unit in the minimum period of time without the use of any special tools. In the AES computer-adapter packaging configuration, it was decided that all the modules were to be designed as pluggable units. Each would have a connector on its mating face. The AES equipment is basically divided into five major modules: logic circuits, memories, power supplies, filters, and interface drive circuits. All these modules will be designed as hermetically sealed units. Similar units, filled with a nontoxic gas, have been extensively used in the IBM designed B-52 bombing-navigation equipment.

All the logic circuits such as timing, control register, and arithmetic logic, will be mounted on a page similar to the ones used in the Saturn-V Launch Vehicle Digital Computer. The page will be slightly larger, measuring 4 inches square and will be mounted on a 200-pin connector. This assembly will then be covered with a can and joined hermetically with a tear strip. The tear strip has been successfully used in the B-52 aircraft electronic equipment. The tear strip concept lends itself to manufacturing checkout, testing, and depot repair.

The sealed can could be made out of either stainless steel or aluminum. Before a recommendation is given, trade-offs would be made of heat transmission, weight, corrosion, and cost. The canned pages will be packed with silicon grease, RTV, or sylgard to prevent moisture penetration. The hermetically sealed cans will be made with guides on each side to assist in aligning the connector and to assist in heat transmission.

Once aligned the page will be mated by a screw action. The screw will be made a part of the page assembly. Its purpose will be to firmly set the connector and lock it into place by means of a camming action. No additional covers will be used.

The power supplies and filter will be approximately 4-inch cubes. Power supplies will be hermetically sealed in either stainless steel or aluminum cans. Modules will be made self-aligning. They will be secured into place either by a screw-cam affair similar to the logic pages, or a ball-type camming arrangement will be used. End item design will depend on size, weight, and accessibility in the vehicle.

Three double density memories will be required. The memories will be approximately 6 x 5-1/2 x 4-inches in size and will be mated in position using a scheme similar to that used for the power supplies. Repairability will be the prime factor in deciding a packaging concept. This is due to the high cost of the memories.

The present design has all modules mounted on the top face of a chassis. Integral cooling, similar to that used for the Saturn-V LVDC, will be used. The bottom face of the chassis will contain the interconnection wiring. The bottom section will be hermetically sealed. The estimated weight of the entire package is 69 pounds.

The present packaging configuration, discussed in the preceding paragraph, may be slightly altered when the vehicle mounting and installation requirements are more completely defined. At present, the package will be installed face up, rack-and-panel style. Other packaging configurations can be used, i.e., a page type package hinged on one side or a spindle package mounted in a merry-go-round style. All these form factors will be fully considered in the final design when requirements are fully defined.

### 1.5 Module Size

Every consideration was given to designing the computer as compactly as possible without sacrificing the maintainability and reliability of the equipment. The present data processing equipment consists of two pieces of hardware, a computer unit and a data adapter unit. Every attempt in this program was made to combine the equipment into one unit and still have a small, light unit.

The AES computer and data adapter consist of memories, power supplies, filter, logic pages, and drive circuits. Every effort was exerted to combine circuits for minimum package density. Different machine packaging trade-offs, were considered. It is envisioned that the computer will be fabricated with integrated circuits; however, it can be made applicable to the present ULD circuit family.

One significant parameter which is frequently used in machine packaging trade-offs is the ratio of required module (page) interconnections per circuit (ULD, flatpack, etc.). Figure 13 shows the results of available data on this parameter for Saturn-V and for the average of other technologies including integrated circuits. Both curves show a general trend that the ratio decreases rapidly as the packing density increases up to about 50 circuits per module and then tends to level off.

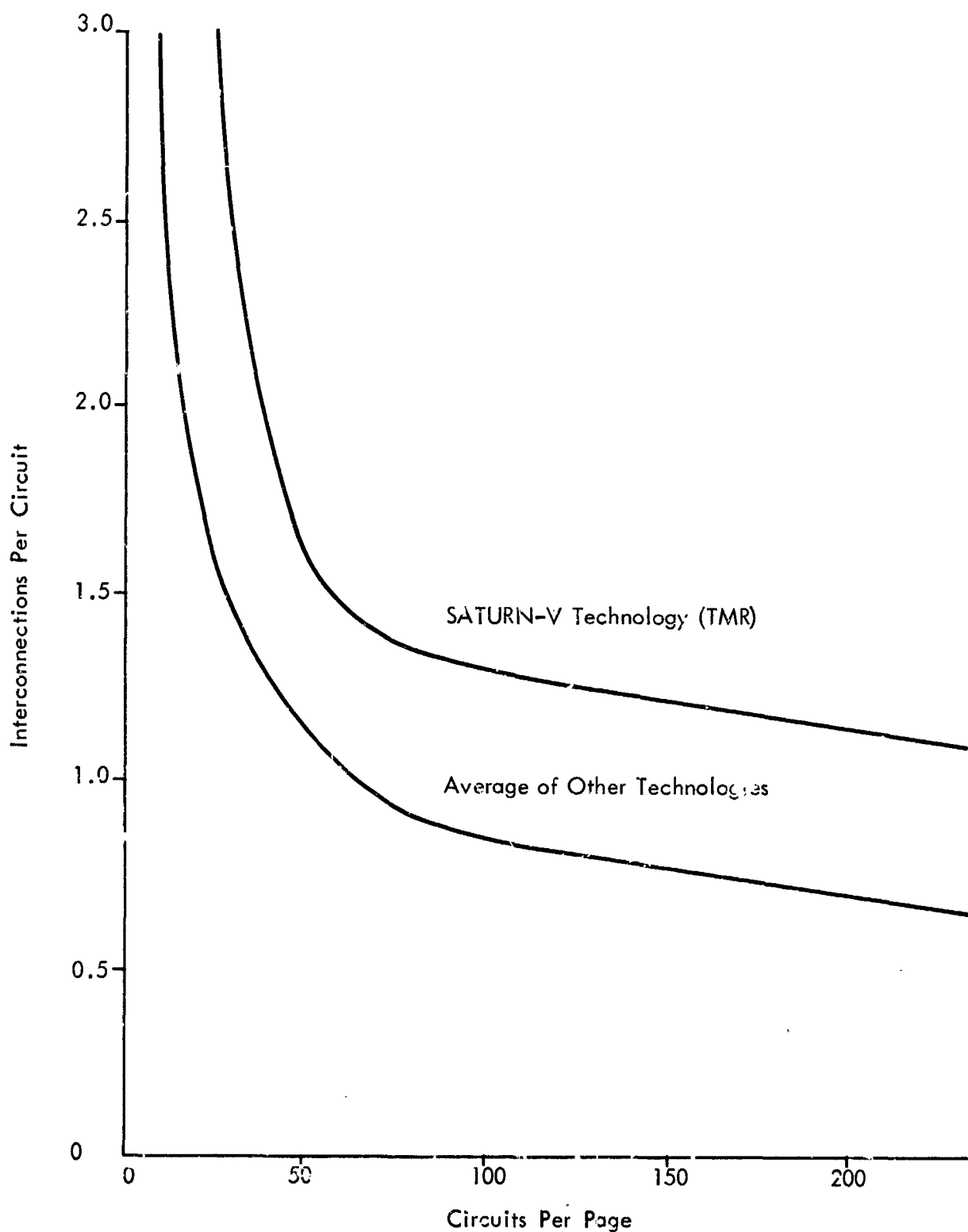


Figure 13. Interconnections per Circuit Versus Circuits per Page

The total number of pluggable interconnections of a machine can now be found for any packing density (circuits per page) by multiplying the total number of machine circuits by the interconnection per circuit value for that packing density.

The curves of Figure 13 indicate that consideration for the total number of pluggable interconnections places a lower limit on the packing density. That is, interconnections limit the module size to some minimum number of circuits per module. The vertical displacement of the Saturn-V curve from the average is due to the reliability requirement of the TMR machine as well as to the difference between Saturn technology and integrated circuit technology. In general, redundancy techniques should increase the number of circuits per page to provide an area sufficiently large enough to accommodate a reasonable block of logic.

The curves in Figure 13 were found to be similar to recently published curves by Meade and Geller<sup>1</sup> and by Keyes<sup>2</sup>. They showed the relation which has been found to hold using SLT technology between the number of connecting pins in a part of a computer such as a card, board, or chassis and the number of logic blocks contained in the part. The curve is reproduced as the solid line in Figure 14. Two observations were made.

The first observation is illustrated by the dotted line in Figure 14. The dotted line represents the ratio of surface volume of a sphere,  $S = \pi^{1/3} 6^{2/3} V^{2/3}$ , when an interconnection is regarded as a unit of surface and a logic block as a unit of volume. These relations are almost identical. It is as though the logic blocks were closely packed into a sphere and connections made to those blocks that were on the surface. It appears that computer interconnections have an essentially three-dimensional character.

The second observation is based on the fact that the human eye contains about  $10^8$  photoreceptors. It is connected to the brain by an optic nerve which contains about  $10^6$  fibers. The point ( $10^6$  connections), ( $10^8$  logic blocks) falls on the extrapolated curve of Meade and Geller. It seems quite reasonable to regard a nerve fiber as a connection. The relation of a photoreceptor to a logic block is less clear. It may be, however, that the amount of data processing which takes place in the eye is about what a computer designer would have put there.

<sup>1</sup> R.M. Meade and H. Geller, "Solid State Design," 6, (7), 21 (July 1965).

<sup>2</sup> Robert W. Keyes, "On the Relation Between Number of Connecting Pins and Number of Logic Blocks," 28 July 1965.

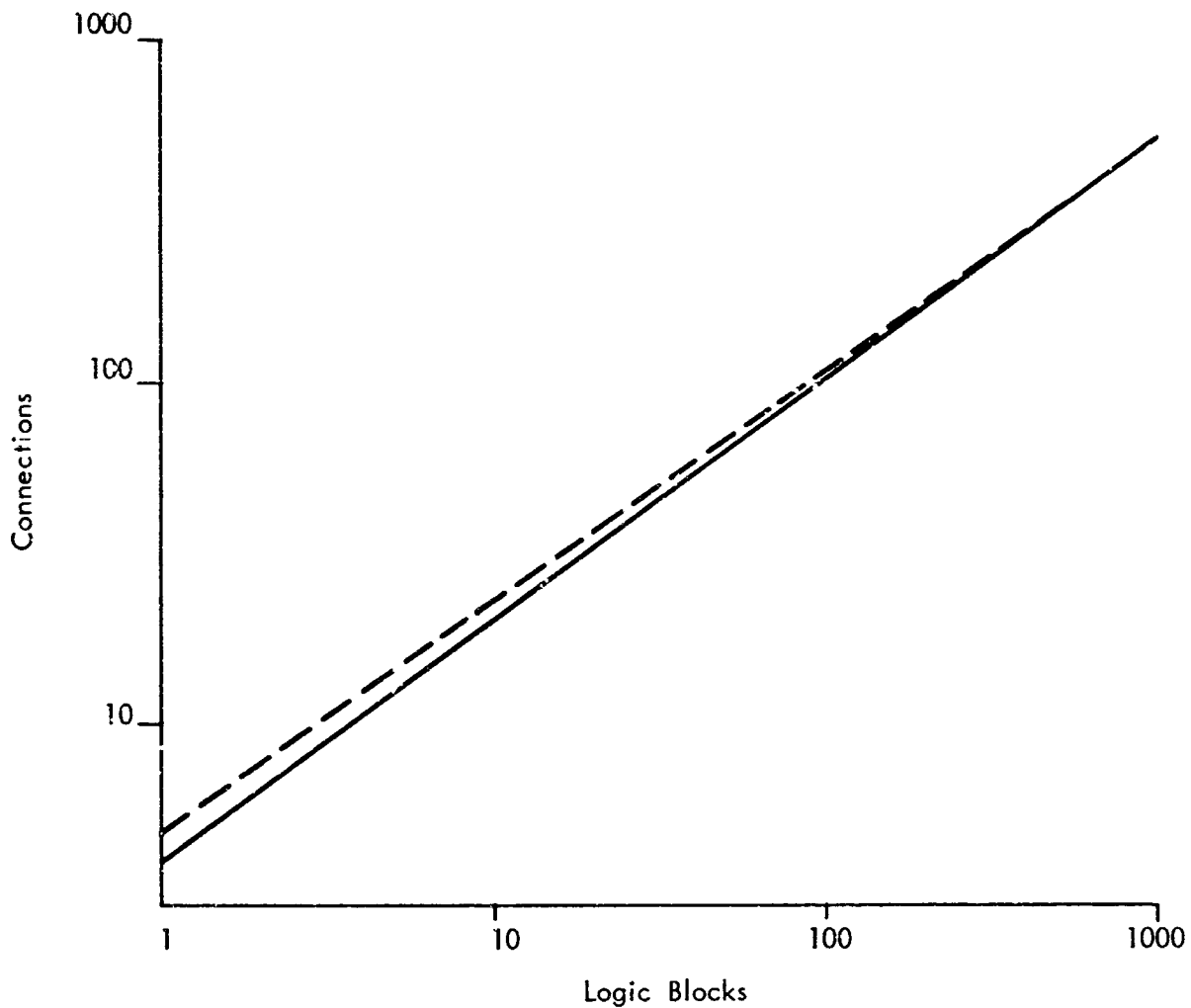


Figure 14. Connections Versus Logic Blocks

Taking this information and interfacing it with Figure 13 results in Figure 15. The dotted curve shows the ratio of surface to volume plotted on Figure 14, and it falls in between Saturn-V technology and the average of other technologies. It also shows that the ratio decreases rapidly as the package density increases up to about 50 circuits per module and then tends to level off.

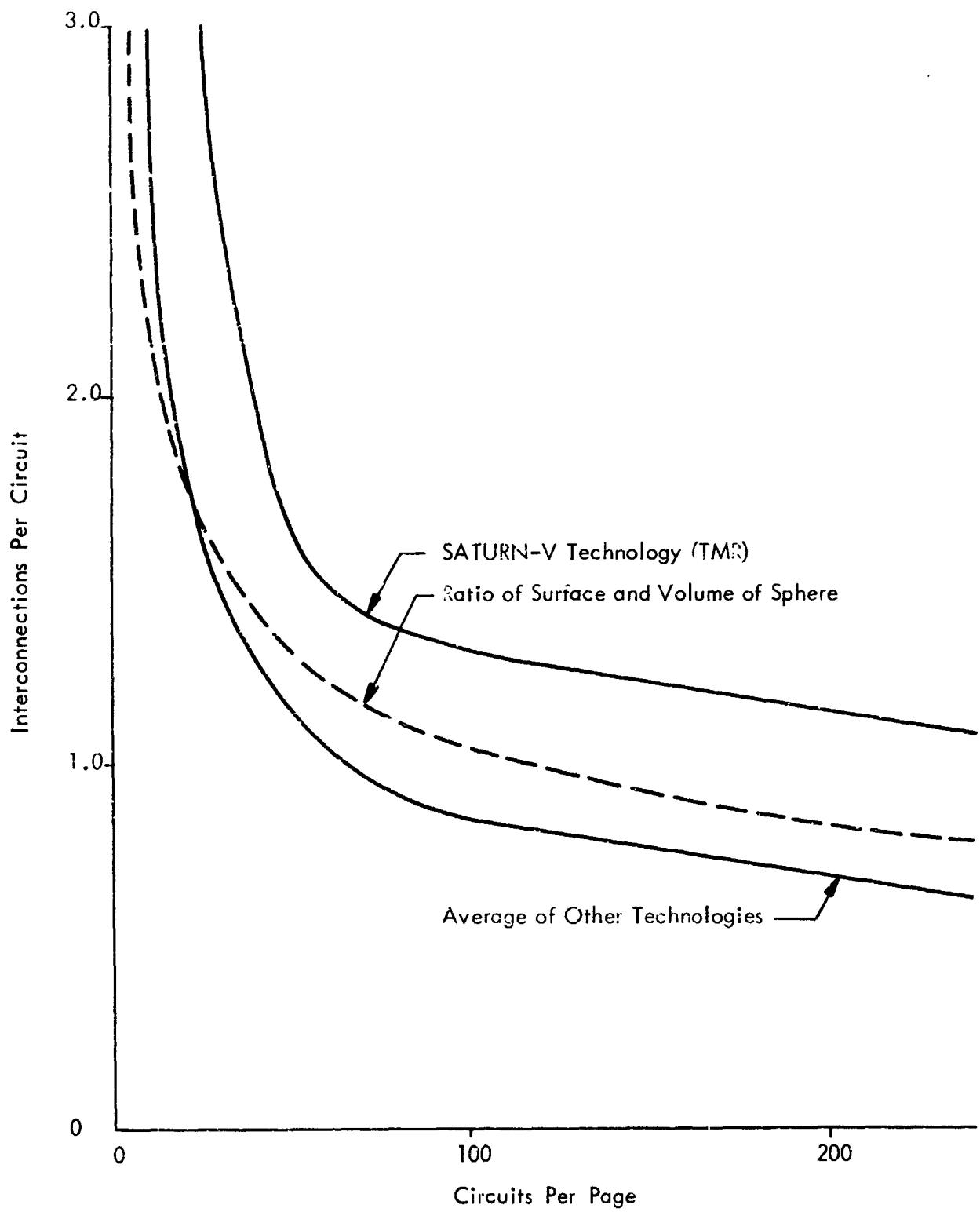


Figure 15. Interconnections per Circuit Versus Circuits per Page

The placement of voters in a TMR machine is an important consideration in machine organization. Maximum machine reliability is theoretically obtained with an organization in which the voting level is such that the reliability of the voter is equal to the reliability of the logic being voted upon. However, in practical aerospace machines, the fan-in and fan-out complexity makes voter placement according to this simple rule far from obvious, especially with restricted packing densities.

A normalized curve of voters per machine versus packing density is given in Figure 16. Although this curve was derived from Saturn data, it should apply generally to other advanced technologies. The curve was constructed according to the rule that voters would be placed on all intermodule signals.

The minimum packing density was taken as the inverter level, point 1 on Figure 16. That is, each inverter is packaged individually as a replaceable module, along with associated AND's and OR's, and the number of voters is equal to the number of inverters in the machine. The ordinate at this point is about 0.75, the ratio of inverter circuits to total circuits in the machine. As the size of the replaceable module is increased to include more inverters, the number of voters required decreases relatively slowly at first because most inverter outputs fan out to several other modules. As these small modules are absorbed into larger modules, the number of inverters feeding out of the module decreases rapidly, and the curve decreases accordingly. Then, in the density region of about 0.05 to 0.10 circuits per page (that is, each replaceable module contains from 5 to 10 percent of the total machine logic), the curve flattens out as the organization tends toward "isolated" functional modules. As the machine organization progresses from ten towards one module per machine, the curve linearly approaches point 2 where the number of voters required has reduced to the logic interface (memory and input-output).

One of the costs of organizing a machine into individual replaceable modules is the increased circuitry required. This increase is due primarily to the additional drivers and decreased circuit-sharing imposed by the modular design. The effect is small except for organizations in which the machine is broken into ten or more modules, as shown in Figure 17.

Figure 17 is a normalized curve of circuits per machine versus circuits per page derived from Saturn-V computer design data. The conclusion from this curve, if it represents the general case and not just Saturn, is that the AES computer should be organized into ten or less modules.

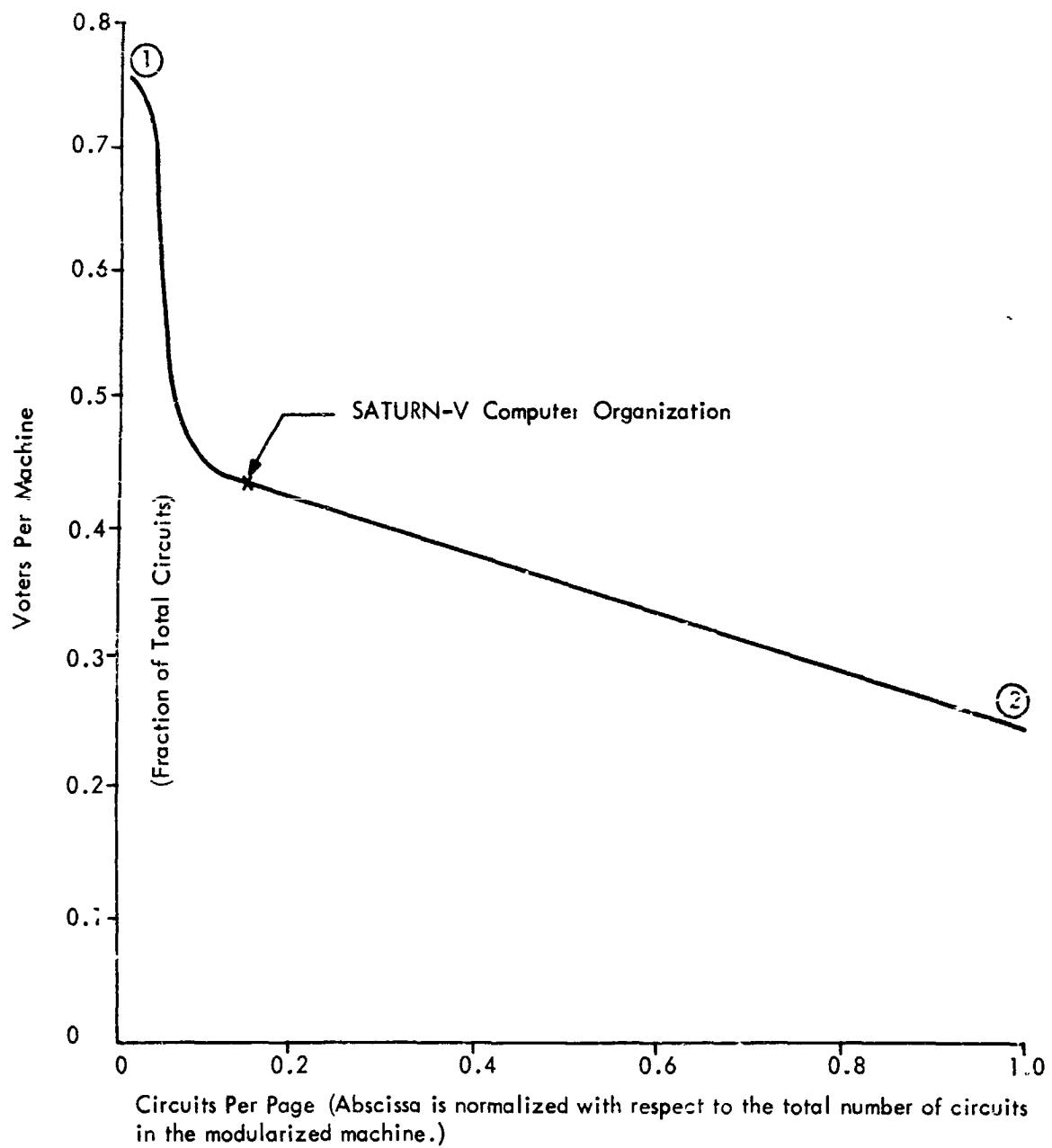


Figure 16. Voters per Page Versus Circuits per Page

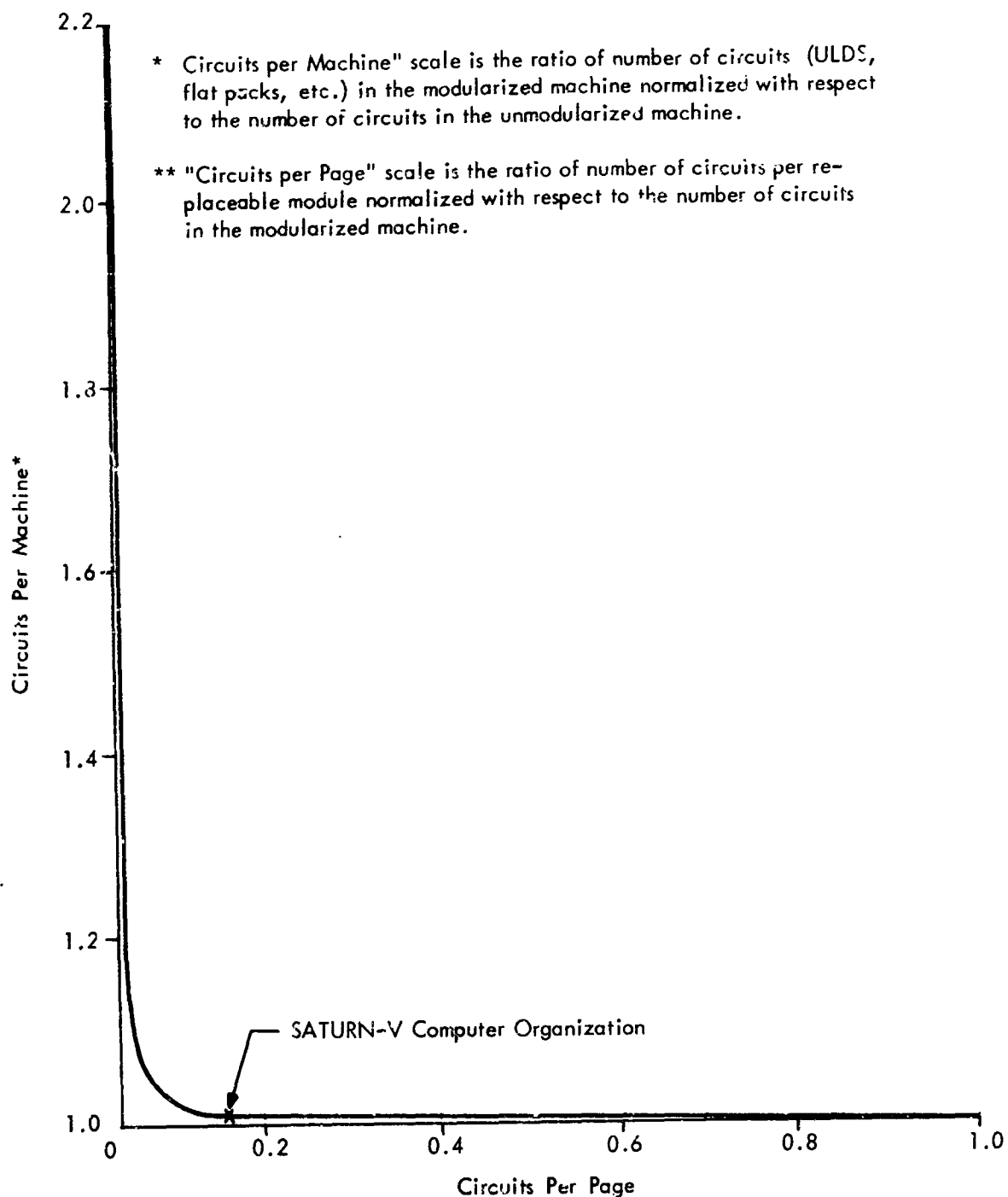


Figure 17. Circuits per Machine Versus Circuits per Page

A TMR machine organization in which all three channels are routed through the same physical replaceable modules has been found to result in the minimum interconnection requirements. This is shown in Figure 18, which represents output voters for module 1 of a TMR computer. If the individual channels of module 1 are packaged on separate physical pages, then the cross-channel communication is external to the page and two inputs and two outputs are required per channel, as shown, or a total of 12 interconnections are required in all. If, on the other hand, the three channels are routed through the same page, then the cross-channel communication signals are internal to the page and only one output is required per channel, or a total of three interconnections in all.

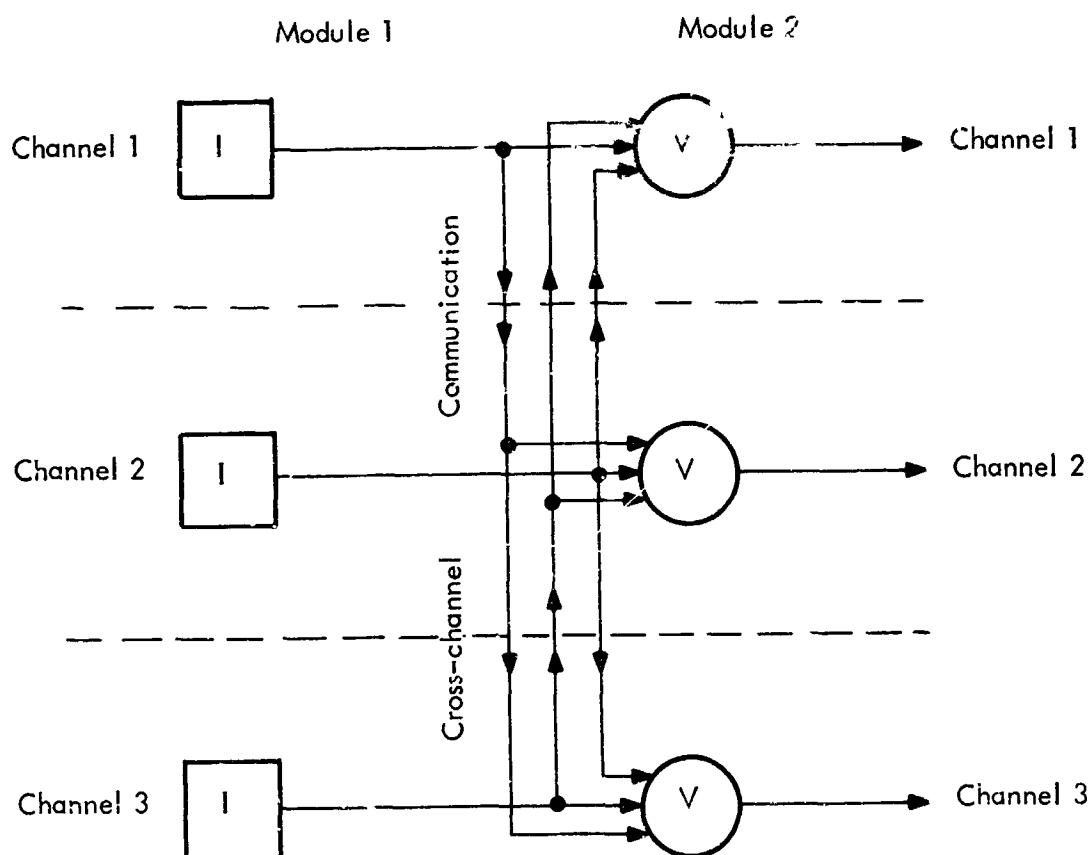


Figure 18. Channel Packaging

The reduction in interconnections which can be realized on the computer level by packaging all three channels on the same physical page has been found to be as high as 25 percent over those required by packaging the channels individually. The feasibility of packaging partial trios (more than one but less than three channels per page) has been investigated and found to offer little advantage over either single-channel or triple-channel packaging.

A preliminary machine organization for the TMR computer assumed ten modules (about the knee of each of the curves of the figures) of about the same size. The resulting module size was about 40 circuits of logic, which increases to 60 as the required drivers and voters are added. Packaging all three channels on the same page results in a packaging density of 180 circuits per page and 160 input-output terminals.

Since the latter number is not compatible with a 98-pin connector, a higher capacity connector must be designed or a replaceable module design containing more than one connector per page must be derived. The first solution is feasible but will result in an appreciable increase per machine in the total number of circuits, voters, and interconnections. The second solution seems feasible at this time after discussing the problem with connector manufacturers. The use of lubricants also assists in fabricating connectors with 200 pins. The third solution is feasible, nevertheless, it does increase alignment problems.

Since the interconnection limitation imposed by the 98-pin capacity of the Saturn-V page connector appeared to be a very severe constraint on the machine reorganization configuration, a quick survey of the connection lubrication state-of-the-art was made to determine if lubrication techniques might allow higher capacity connectors to be used. The results of a continuing study at IBM of the characteristics of thin film lubricants to reduce contact wear were reviewed. Consideration was also given to the possible use of lubricants as protective coatings for contact surfaces in adverse environments.

A lubrication study by the U.S. Army Electronics Laboratories and Stanford Research Institute resulted in the recommendation of octadecylamine-hydrochloride (ODA-HCL) for use with gold contact surfaces. Tests at IBM have verified the excellent properties of this lubricant. Octadecylamine-hydrochloride lubricant forms a very stable and tenacious film on gold surfaces. These properties are probably due to physical absorption of the lubricant by the gold surface, and perhaps also due to electrostatic attraction between the lubricant and the gold. The thin film does not affect the electrical resistance of the

gold contact while decreasing its coefficient of friction up to 75 percent. The films are stable with time, contaminants, and hard vacuum. The film maintained its lubricating properties and its low electrical resistance characteristics after prolonged exposure of several weeks to atmospheres containing sulphur dioxide, hydrogen sulfide, and water vapor.

Since the test results on octadecylamine-hydrochloride were so consistently encouraging, it is recommended for AES connector lubrication applications, even if small capacity connectors are used. The decrease in insertion forces which it apparently affords, however, would seem to indicate that page connectors with capacities of at least 150 to 200 pins may well be feasible.

## 2.0 MACHINE ORGANIZATION

The machine organization of the Saturn-V computer and the Apollo backup data adapter was examined to determine its applicability to the critical phases of the mission as well as its applicability to in-flight maintenance during the noncritical phases of the mission. Considerable study effort was then expended on modifying those areas of the machine organization representing serious constraints on the mission capabilities of the computer and data adapter. The reorganized version of the computer system included major changes in the oscillator, memories, power supplies, power, and timing distributions, and internal grounding. A TMR/simplex mode was developed which incorporates certain automatic switching features and provides appreciable increase in reliability over the basic TMR mode. A portion of the organization study was directed at reducing the susceptibility of the computer system to externally generated voltage transients.

### 2.1 TMR Characteristics

One of the primary objectives of this study was to determine the feasibility of a triple modular redundancy configuration as a solution to the short-term reliability problem in AES missions. TMR is a form of redundancy incorporating two-out-of-three voting as shown in Figure 19. Even if one module fails (dotted lines), the outputs of all three voters are correct. The TMR organization therefore possesses the unique characteristic that component failures can be tolerated and their disruptive effects on system performance masked automatically by voting without the need for error detection, diagnosis, and repair. This error masking occurs without interruption of the operational program, a characteristic found in few other forms of redundancy.

The reliability models for the TMR portions of the computer configurations examined during this study were based on the following analysis of the reliability states of a TMR module. A TMR module is defined as a section of the instrumentation isolated from other sections by voters. In the computer configurations of this study, this reliability module corresponds generally to the physical modules since most of the voters were used at the physical interfaces.

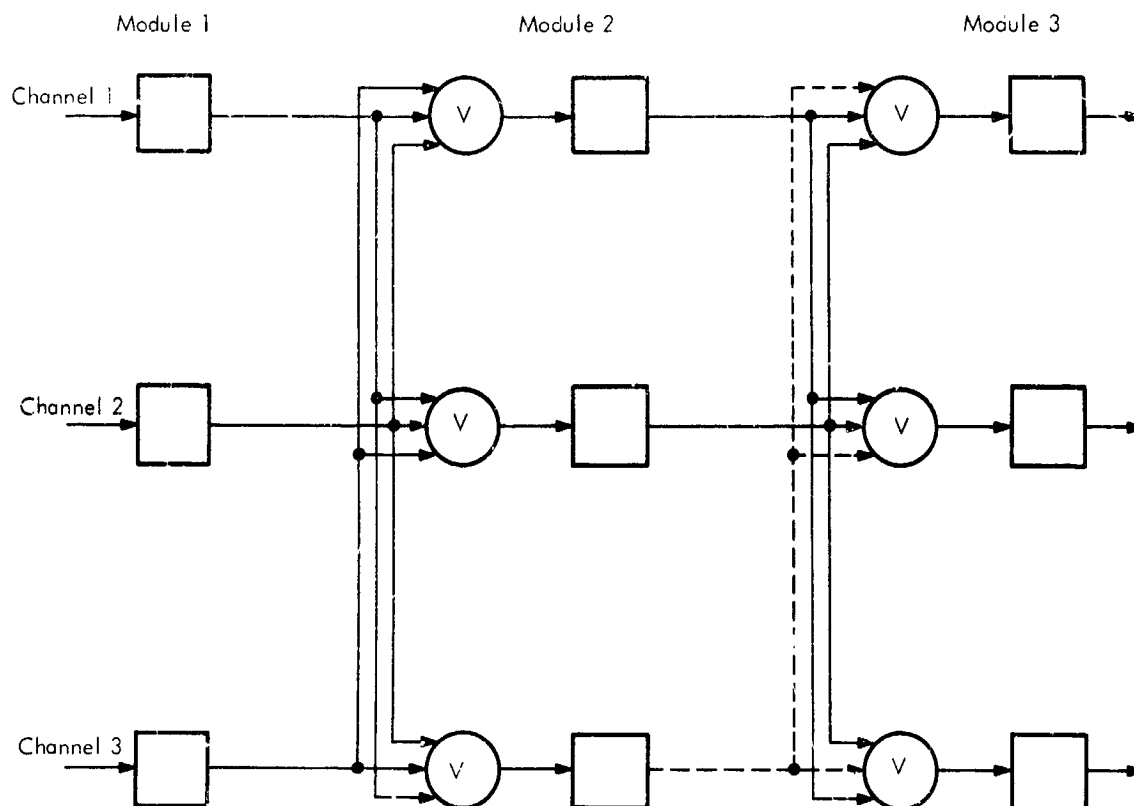


Figure 19. TMR Voting

### 2.1.1 Reliability States

The primary reliability states of a TMR module are shown in Table 3. State 1 represents the condition of all channels operating. State 2 represents the condition of two channels operating and one failed. The coefficient 3 indicates that there are three ways the module can be in State 2: channel 1 or channel 2 or channel 3 failed. State 3 represents the condition of one channel operating and two failed, and State 4 represents the condition of all three channels failed.

States 1 and 2 are operating states and state 4 is a failed state. State 3, however, can be operating or failed depending on whether the failures in the two failed channels are in the opposite or in the same logic direction, respectively. If one channel is failed to a logic "zero" and the second channel failed to a logic "one", for example, the third channel dominates the voting and the system will continue to operate correctly.

TABLE 3 - Reliability States for TMR Modules

State	Operating	Failed
1	$R_c^3$	
2	$3 R_c^2 (1 - R_c)$	
3	$3 P(o) R_c (1 - R_c)^2$	$3 P(s) R_c (1 - R_c)^2$
4		$(1 - R_c)^3$

State 1 - All modules operating

2 - One module failed

3 - Two modules failed

4 - Three modules failed

P(o) - Probability that the two failures are in the opposite logic direction

P(s) - Probability that the two failures are in the same logic direction

$R_c$  - Reliability of one channel of the TMR module.

### 2.1.2 Basic TMR Reliability

The basic reliability of a TMR module is derived by adding the probabilities of the operating states. From Table 3, the reliability of the TMR module is:

$$R_{TM} = R_c^3 + 3 R_c^2 (1 - R_c) + 3 P(o) R_c (1 - R_c)^2$$

where  $R_c$  is the reliability of one channel of the module and P(o) is the conditional probability that, if two failures occur, they occur in opposite logic directions and their votes therefore cancel.

Module reliability is plotted against channel (or simplex) reliability in Figure 20 for three values of P(o). Note that TMR redundancy actually provides less reliability than simplex if the reliability

$$R_{tm} = R_c^3 + 3 R_c^2 (1 - R_c) + 3 P(0) R_c (1 - R_c)^2$$

$R_{tm}$  = TMR Module Reliability

$R_c$  = Simplex (Channel) Module Reliability

$P(0)$  = Probability that two failures will occur  
in opposite logical directions

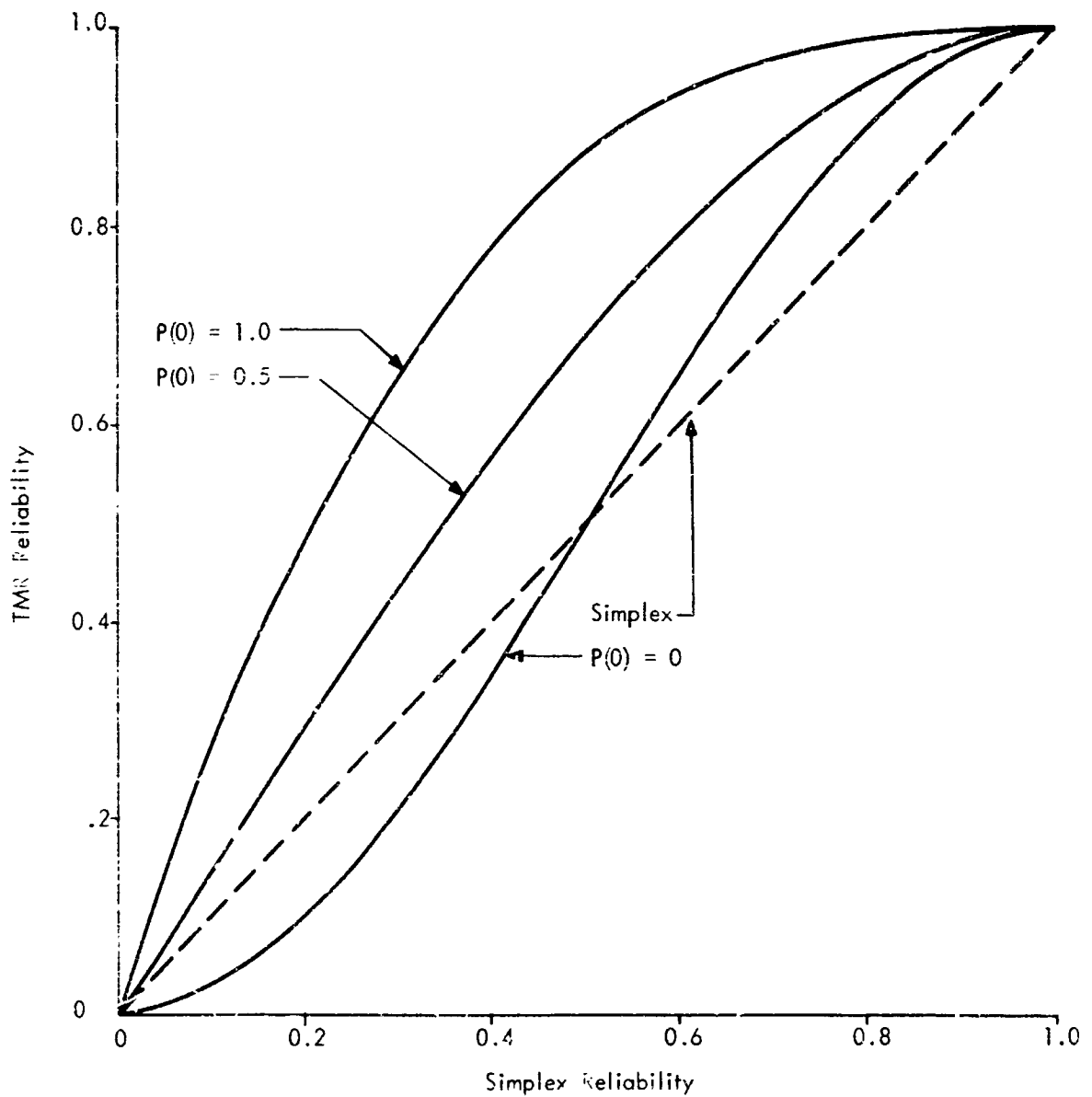


Figure 20. TMR Versus Simplex Reliability

of the simplex channel is less than 0.5 and if it is assumed that all related logic failures occur in the same logical direction. This conservative assumption is usually made in estimating the reliability of actual TMR systems such as the Saturn-V computer and data adapter. The assumption of equal probability of failure to "one" or "zero" states would be applicable to a system constructed of symmetrical double-line-transfer logic, but such systems rarely exist in practice since circuit minimization requirements normally dictate an appreciable amount of unsymmetrical single-line-transfer logic.

#### 2.1.3 Intermittent Masking

In the case of intermittent failures in a TMR module, the effects of the failure are voted out as in the case of solid failures, but when the period of the intermittent ends, the module automatically recovers its original reliability state. This automatic recovery is a unique characteristic of TMR system organizations and a few isolated subsystem units such as the duplex Saturn-V memories. Flight failures on present and past programs tend to be mostly intermittent in nature, probably because of the much higher screening efficiency of present checkout methods for solid faults than for intermittents resulting in most of the solid faults being corrected before flight. In fact, as the level of testing progresses from preassembly screening of modules to preflight checkout of computer systems, the ratio of intermittent to solid failures found during test apparently increases monotonically with time and usage.

Data relating to failures detected in past computers from acceptance testing through end-use indicate that over 30 percent of the expected AES computer failures would be masked and would not degrade reliability. Although some rough calculations of the increase in reliability estimates due to consideration of the failure mechanisms of intermittents in TMR organizations were made in the preproposal study, this item was not pursued further during the study. All failures were assumed solid, and the reliability estimates are therefore conservative.

#### 2.1.4 Channel/Module Switching

Channel and module switching capabilities are provided in the Saturn-V computer and force the computer to operate in a simplex mode. Channel switching forces the computer to operate on any one of the three simplex channels while module switching allows mixed

channel operation. In either case, the operating channel is selected by setting one voter input to a logical zero and a second voter input to a logical one so that their "votes" cancel and the third input determines the voter output. Channel switching is shown in Figure 21 and module switching is shown in Figure 22. The heavy lines indicate the selected data paths in both figures.

The Saturn-V voter is shown logically in Figure 23. Normally inputs A1, A2, and A3 and outputs CH1, CH2, and CH3 are all alike (all zeros or all ones). Points A, B, and C (inputs to the logic elements driving the voter) are connected to +6 volts, and points D, E, and F are connected to +12 volts. To select channel 1 (CH1), inputs A2 and A3 must be set to a logical one, input E to a zero, and input F to a one. Inputs E and F could be reversed. Outputs CH1, CH2, and CH3 now correspond to input A1 because the threshold of the current summers are set for two units of current; A3 supplies one unit, A2 supplies none, and the state of A1 therefore determines whether the current threshold of the voter is reached or not.

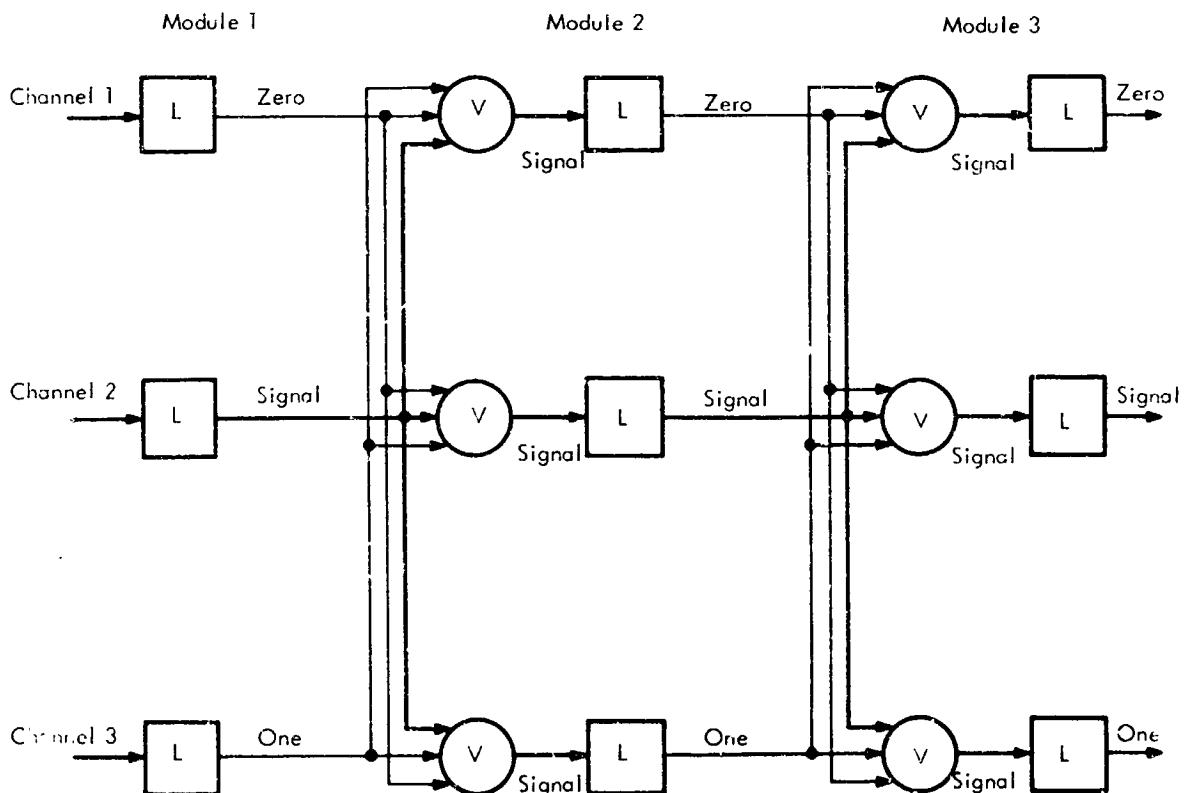


Figure 21. Channel Switching

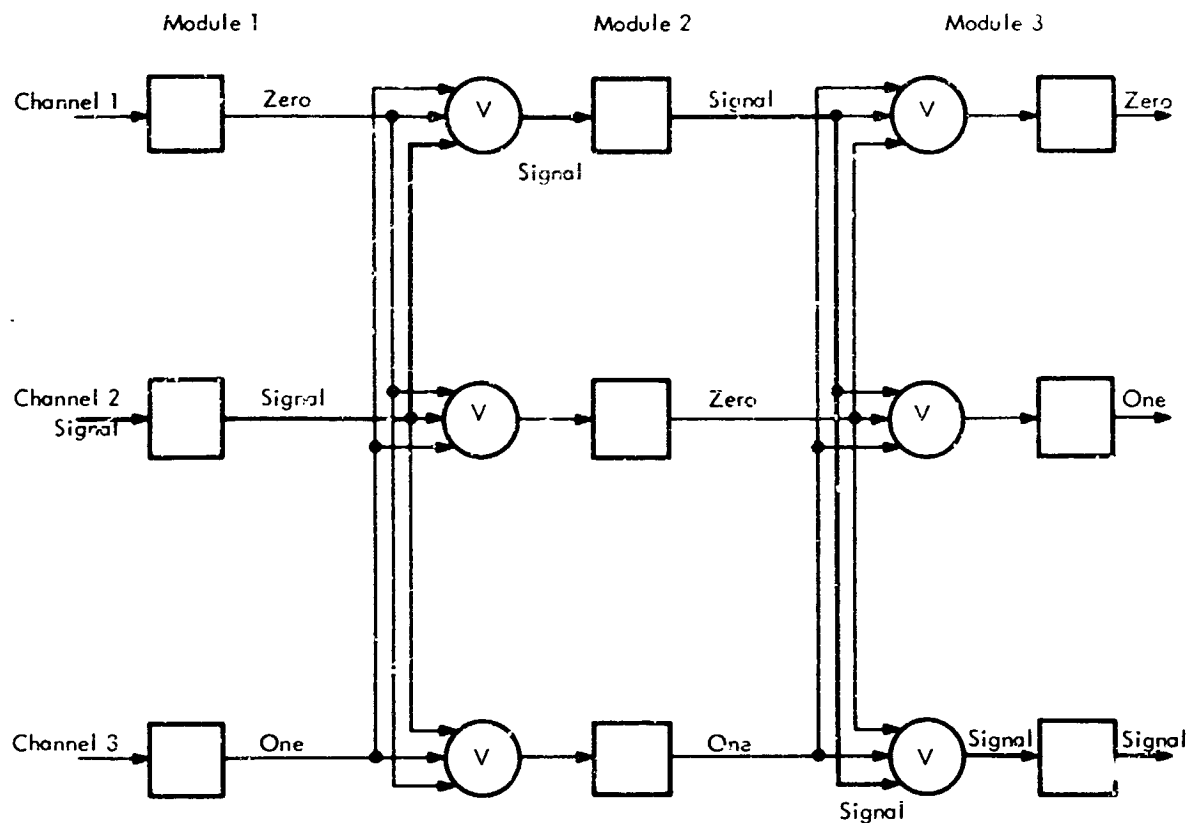


Figure 22. Module Switching

## 2.2 Trade-off Criteria

Any system optimization effort will involve trade-offs among mutually conflicting parameters or criteria. The machine organization trade-offs of this study involved considerations of reliability, error detection and fault isolation, module replaceability and sparing, machine size and complexity, and susceptibility to transients. The last criteria dictated reinstrumentation of simplex and duplex components of the Saturn-V computer and Apollo backup data adapter to TMR (with special consideration for memory protection) and did not conflict with the trade-off criteria.

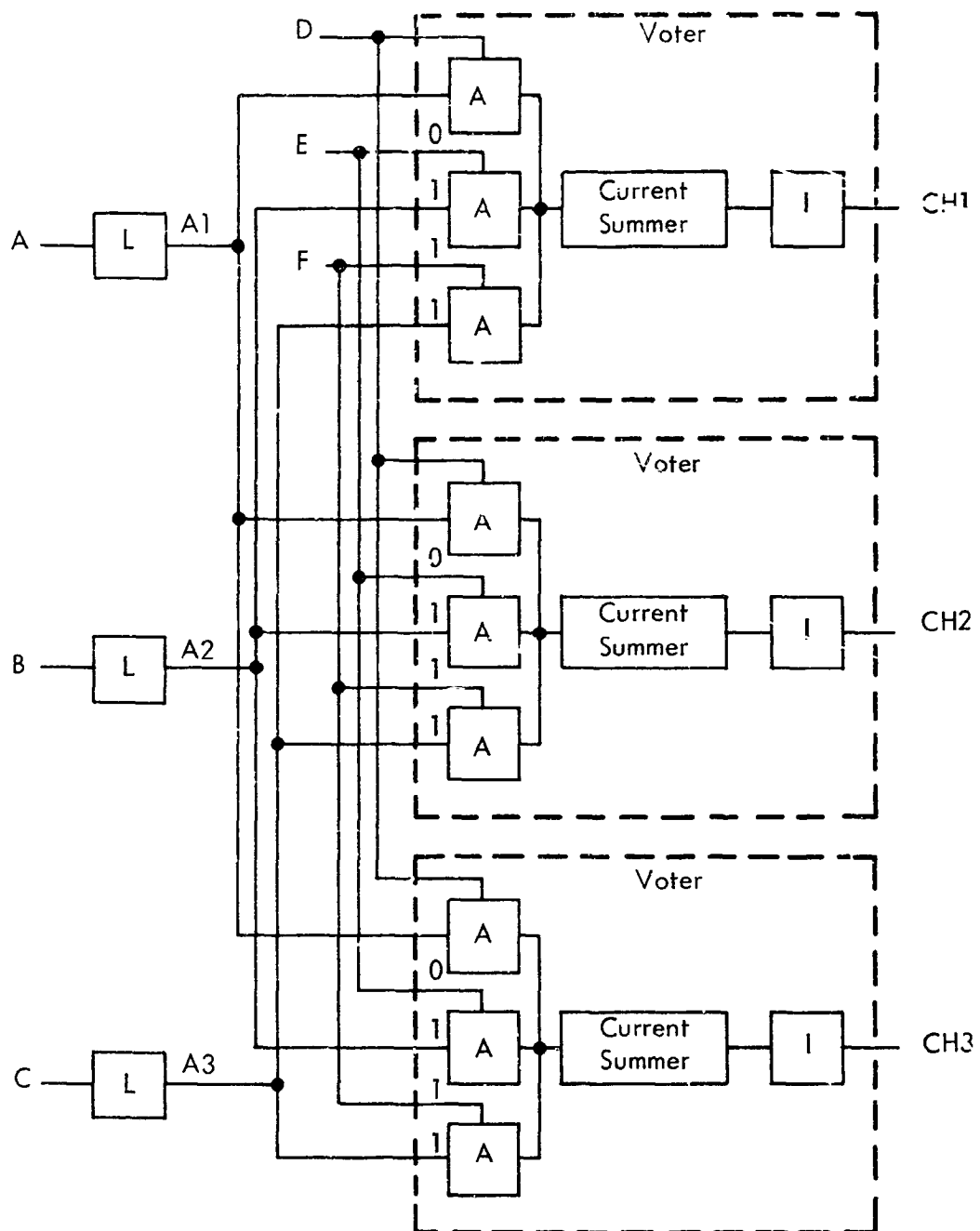


Figure 23. Saturn-V Voter

Reliability, maintenance, and size criteria were mutually conflicting. Reliability maximization dictated that the computer system be partitioned into small modules at a logic level where the reliability of the circuits being voted is equal to the reliability of the voter. The requirement for automatic failure isolation, however, dictated that the computer system be partitioned into functional modules (such as arithmetic or timing). The minimization of circuits and interconnections could be achieved only with a completely unmodularized computer system.

After some consideration of these conflicting requirements, it was decided to ignore reliability as a trade-off criteria until partitioning of the machine was completed on the basis of maintainability and size trade-offs, and then to test the reconfigured machine to determine whether the reliability requirements of the AES-EPO mission could be satisfied with that configuration. In addition, preliminary examination of the relationship between machine size (number of components or circuits) and modularization level showed that relatively little increase in size occurred as the machine was partitioned into larger numbers of modules up to about ten, beyond which the size increased very rapidly. The optimization studies of machine partitioning therefore were based on maintainability criteria alone (since these criteria dictated less than ten modules).

Error detection and fault isolation dictated a functional partitioning of the computer system which also satisfied the module replaceability and sparing requirements.

## 2.3 Basic Subsystem Configuration

The basic system upon which the study was based consisted of the TMR Saturn-V computer and a redundant version of the Apollo backup data adapter. This basic system was examined to determine to what extent it could meet the functional and availability requirements of the 90-day AES-EPO mission and where redesign was necessary. Special attention was given to the reliability and failure isolation capabilities of the basic computer and data adapter.

### 2.3.1 Saturn V Computer Description

The computer information flow is illustrated in Figure 24. This simplified block diagram depicts the major data flow paths and associated register level logic. The timing logic and input/output (I/O) section are not shown.

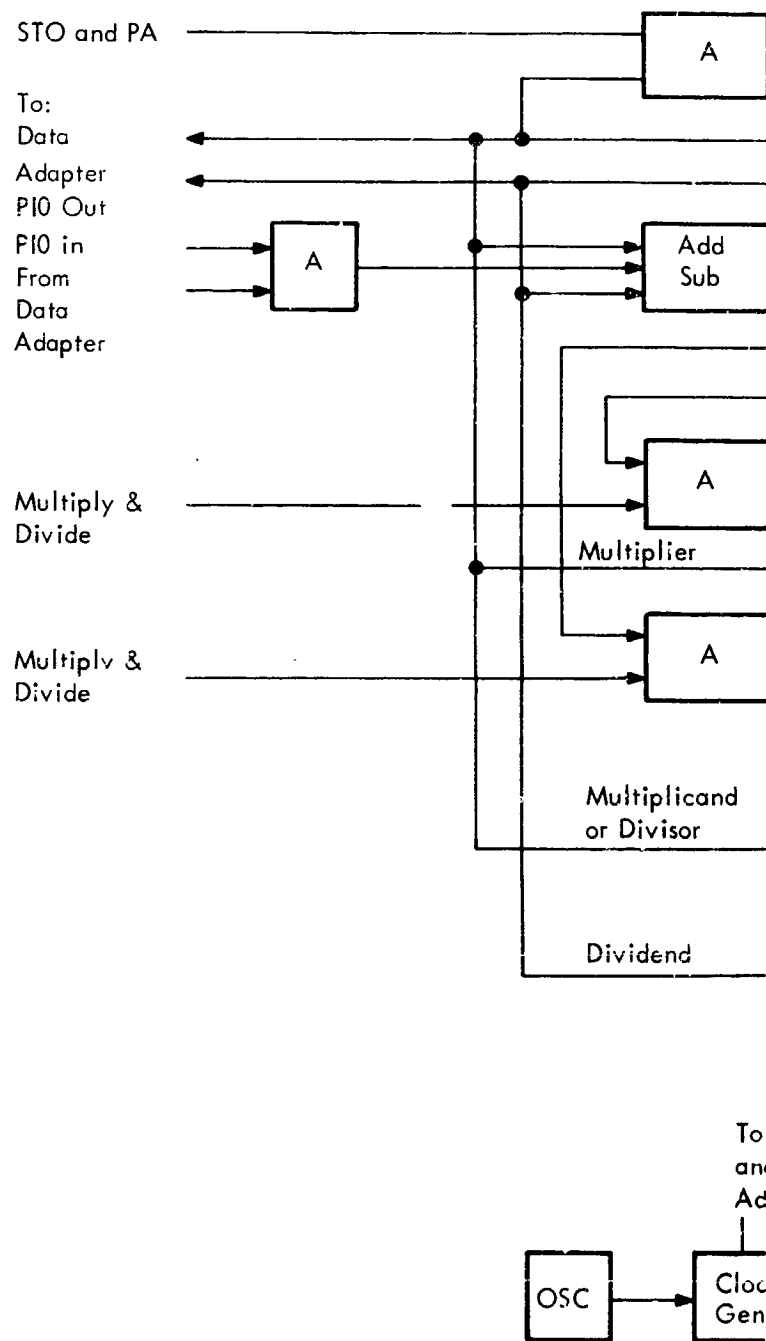
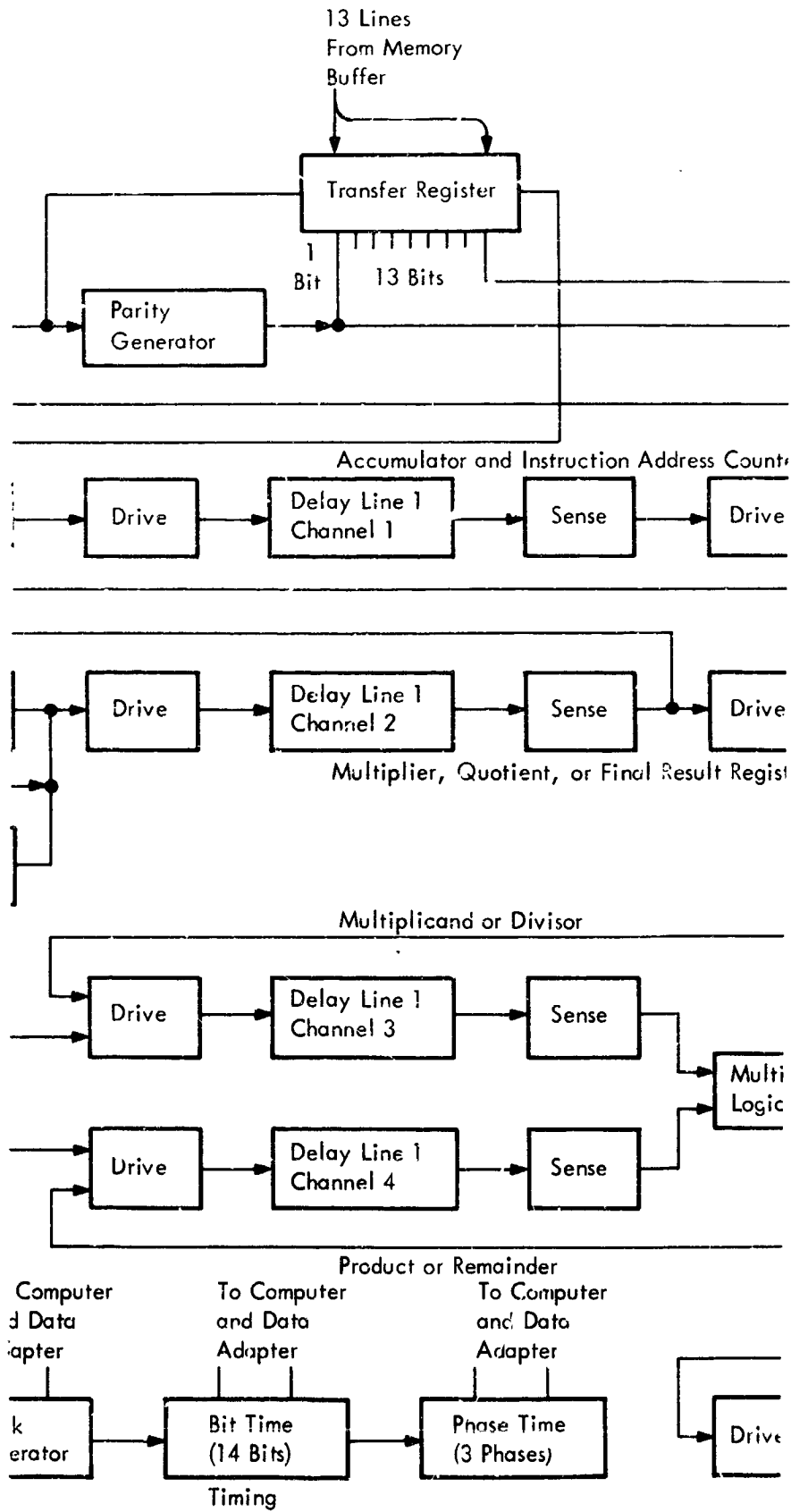
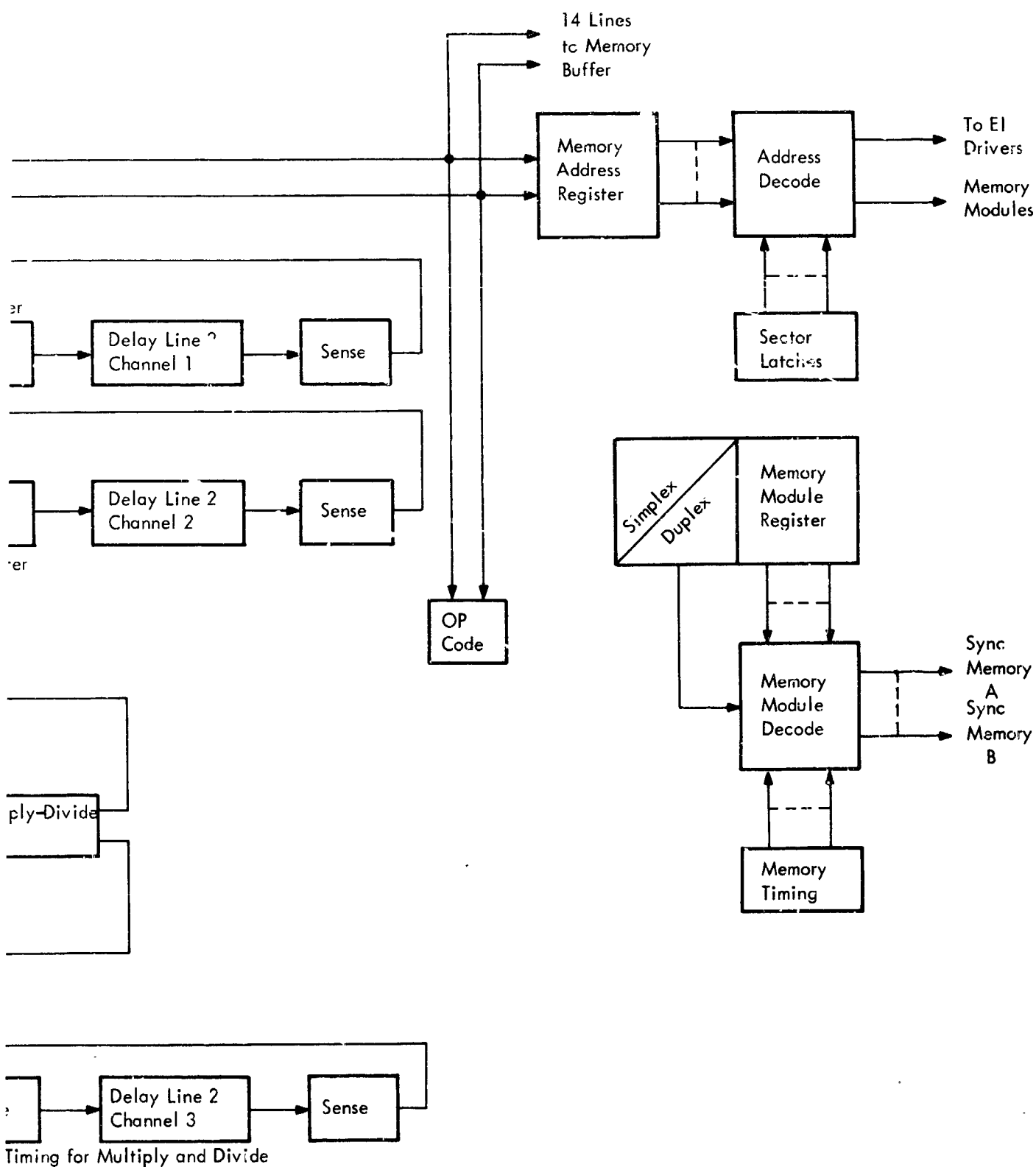


Figure 24. Saturn-V Guidance Computer





The computer is a serial, fixed-point, stored-program, general-purpose machine which processes data using "two's complement" arithmetic. Two's complement arithmetic obviates the recomplementation cycle required when using "sign plus magnitude" arithmetic. Special algorithms have been developed and implemented for multiplication and division of two's complement numbers. Multiplication is done four bits at a time and division two bits at a time.

A random-access magnetic core memory is used as the computer storage unit. A serial data rate of 512 kilobits per second is maintained by operating the memory units in a "serial-by-byte, parallel-by-bit" operating mode. This allows the memory to work with a serial arithmetic unit. The parallel read-write word length of 14 bits includes one parity bit to allow checking of the memory operations.

Storage external to the memory is located predominantly in the shift register area. High reliability in this area is achieved by using glass delay lines for arithmetic registers and counters.

Each instruction is comprised of 4-bit operation code and a nine-bit operand address. The 9-bit address allows 512 locations to be directly addressed. The total memory is divided into sectors of 256 words, and contains a residual memory of 256 words. The 9-bit address specifies a location in either the previously selected sector (data sector latches) or in the residual memory. If the operand address bit (A9) is a binary "0", then the data will come from the sector specified by the sector register; if A9 is a "1" the data will come from residual memory.

Instructions are addressed from an 8-bit instruction counter augmented by a 4-bit instruction sector register. Sector memory selection is changed by special instructions which change the contents of the sector register. Sector size is large enough so that this is not a frequent operation.

Data words consist of 26 bits. Instruction words consist of 13 bits and are stored in memory two-instructions per data word. Hence instructions are described as being stored in syllable 1 or syllable 2 of a memory word. Two additional bits are used in the memory to provide parity checking for each of the two syllables.

The computer is programmed by means of single-address instructions. Each instruction specifies an operation and an operand address. Instructions are addressed sequentially from the memory under control of the instruction counter. Each time the instruction counter is used, it is incremented by one to develop the address of the next instruction. After the instruction is read from memory and parity checked, the operation code is sent from the transfer register to the operation (OP) code register, a static register which stores the operation code for the duration of the execution cycle.

The operand address portion of the instruction is transferred in parallel (9 bits) from the transfer register (TR) to the memory address register. The TR is then cleared.

If the operation code requires reading the memory, the contents of the operand address are read 14 bits at a time (including parity) from the memory into the buffer register where a parity check is made. Data bits are then sent in parallel to the TR. This information is then serially transferred to the arithmetic section of the computer. If the operation code is a store (STO), the contents of the accumulator are transferred serially into the TR and stored in two 14-bit bytes. A parity bit is generated for each byte.

Upon completion of the arithmetic operation, the contents of the instruction counter are transferred serially into the TR. This information is then transferred in parallel (just as the operand address had previously been transferred) into the memory address register. The TR is then cleared and the next instruction is read, thus completing one computer cycle.

The data word is read from the memory address specified by the memory address register and from the sector specified by the sector register. Data from the memory go directly to the arithmetic section of the computer where it is operated on as directed by the OP code.

The arithmetic section contains an add-subtract element, a multiply-divide element, and storage registers for the operands. Registers are required for the accumulator, product, quotient, multiplicand, multiplier, positive remainder, and negative remainder. The add-subtract and the multiply-divide elements operate independently of each other. Therefore, they can be programmed to operate concurrently if desired; i.e., the add-subtract element can do several short operations while the multiply-divide element is in operation.

No dividend register is shown in Figure 24 because it is considered to be the first remainder. The divisor is read from the accumulator during the first cycle time and can be regenerated from the two remainders on subsequent cycles. As indicated, both multiply and divide require more time for execution than the rest of the computer operations. A special counter is used to keep track of the multiply-divide progress and stop the operation when completed. The product-quotient (PQ) register has been assigned an address and is addressable from the operand address of any instruction. The answer will remain in the PQ register until another multiply-divide is initiated.

A limited program interrupt feature is provided to aid the I/O processing. An external signal can interrupt the computer program and cause a transfer to a subprogram. Interrupt occurs when the instruction in progress is completed. The interrupt forces a HOP constant to be retrieved from the reserved residual memory location (octal address 400). The constant designates the start of the subprogram. The instruction counter, sector and module registers, and syllable latch can be stored in a reserved residual memory location by programming a STO 776 on HOP 777 as the first instruction in the subprogram. Automatic storage of the accumulator and product-quotient registers is not provided; this must be accomplished by the subprogram. Protection against multiple interrupts and interrupts during MPY, DIV, HOP, and EXM operations is provided.

The interrupt signal may be generated by a timed source. The rate at which it is generated is controlled by changing the magnitude of a number which is being continually summed. When the summed number reaches a predetermined value, the interrupt signal is generated. This is accomplished in the data adapter.

The main program can be resumed by addressing the contents of residual memory word 776 or 777 with a HOP instruction, after restoring the accumulator and PQ register to their pre-interrupt values.

Certain discrete input signals are allowed to cause interrupt. These are useful in causing the I/O subprogram to give immediate attention to an input or output operation.

The memory for the Saturn-V Guidance Computer uses conventional toroidal cores in a unique self-correcting duplex system. The memory unit consists of up to eight identical 4096-word memory modules which may be operated in simplex for increased storage capability or in duplex pairs for high reliability. The basic computer

program can be loaded into the instruction and constants sectors of the memory at electronic speeds on the ground or just prior to launch. Thereafter, the information content of constants and data can be electrically altered but only under control of the computer program.

The self-correcting duplex system uses an odd parity bit with detection schemes for malfunction indication and correction. In conjunction with this scheme, error-detection circuitry is also used for memory drive current monitoring. Unlike conventional toroid random-access memories, the self-correcting extension of the basic duplex approach permits regeneration of correct information after transients or intermittent failures. Otherwise destructive read-out of the memory could result.

The basic configuration consists of a pair of memories providing storage for 8192 14-bit memory words for duplex operation, or 16,384 14-bit memory words for simplex operation. Each of the simplex memories includes independent peripheral instrumentation consisting of timing, control, address drivers, inhibit drivers, sense amplifiers, error-detection circuitry, and I/O connections to facilitate failure isolation. Computer functions which are common to these simplex units consist of the following:

- Memory address register outputs
- Memory transfer register input-output
- Store gate command
- Read gate command
- Syllable control gates.

The computer functions, which are separate for each simplex memory, consist of synchronizing gates which provide the serial data rate of 512 kilobits per second. This data rate is required by the computer to generate a start memory unit command at 128 kilobits per second. These gates also provide the selection of multiple simplex memory units for storage flexibility and permit partial or total duplex operation throughout the mission profile to extend the mean-time-before-failure for long mission times. Each of the simplex units can operate independently of the others or in a duplex manner. The memory modules are divided into two groups: one group consisting of even numbered modules (0-6) and the other consisting of odd numbered modules (1-7). There is a buffer register associated with each group which is set by the selected modules.

For duplex operation, each memory is under control of independent buffer registers when both memories are operating without failure. Both memories are simultaneously read and updated, 14 bits in parallel. A single cycle is required for reading instructions (13 bits plus 1 parity bit per instruction word). Two memory cycles are required for reading and updating data (26 bits plus 2 parity bits). The parallel outputs of the memory buffer registers are serialized at a 512-kilobit rate by the memory transfer register under control of the memory select logic. Initially, only one buffer register output is used, but both buffer register outputs are simultaneously parity checked in parallel. When an error is detected in the memory being used, operation immediately transfers to the other memory. Both memories are then regenerated by the buffer register of the "good" memory, thus correcting transient errors. After the parity-checking and error-detection circuits have verified that the erroneous memory has been corrected, operation returns to the condition where each memory is under control of its own buffer register. Operation is not transferred to the previously erroneous memory until the "good" memory develops its first error. Consequently, instantaneous switching from one memory output to another permits uninterrupted computer operation until simultaneous failures at the same storage location in both memories cause complete system failure.

Proper operation of the memory system during read cycles is indicated by each 14-bit word containing an odd number of bits and a logical "1" output of the error-detecting circuitry. If either or both of these conditions are violated, operation is transferred to the other memory. During regenerate or store cycles, since parity checking cannot be performed, failure detection is accomplished by the error-detection circuitry only and by parity detection during subsequent read cycles. Intermittent addressing of memory between normal cycles is also detected by the error-detecting circuitry producing a logical "1" output.

A summary of the computer characteristics is given in Table 4.

### 2.3.2 Apollo Backup Data Adapter Description

The Apollo data adapter contains a high speed I/O processor and the input and output circuitry and logic necessary to connect the central processor unit and the I/O processor with the rest of the guidance and navigation equipment. It also contains a data exchange register (DER), which buffers and translates data flowing between the central processor and I/O processor or between the central processor and

TABLE 4 — TMR Computer Characteristics

Function	Description
Type	General purpose, stored program, serial, fixed point binary.
Clock	2.048 Mc clock, 512 kilobits per second information rate.
Speed	Add-subtract and multiply-divide simultaneously.
Add	82 $\mu$ s
Multiply	328 $\mu$ s
Divide	656 $\mu$ s
Memory Type	Toroidal magnetic core, random access.
Storage Capacity	Interconnections provide for using up to eight memory modules having 4096 28-bit words.
Input/Output	External; computer-programmed I/O control. External interrupt provided.
Component Count	40,000 silicon semiconductors and cermet resistors.
Reliability	0.996 probability of success for 250 hours; TMR logic and duplex memories employed.
Packaging	73 electronic page assemblies.
Weight	78.5 pounds.
Volume (Swept)	2.37 cubic feet.
Power	142 watts.

external subsystem interfaces. In general, the central processor directly controls discrete inputs and outputs in the data adapter. The I/O processor stores and generates pulse train inputs and outputs and provides the necessary communication link between these signals and the central processor. It also provides discrete outputs for controlling the spacecraft reaction control system (RCS) jets.

The data adapter is also required to:

- Accept and process interrupt signals to the central processor and I/O processor from within the data adapter and from other spacecraft subsystems.
- Provide continuous timing signals for spacecraft subsystems
- Convert Lunar Excursion Module (LEM) hand controller signals from analog-to-digital form
- Provide regulated d-c power to both the central processor and data adapter
- Provide regulated d-c excitation power for various spacecraft discrete inputs.

A block diagram of the data adapter is shown in Figure 25.

All functions within the data adapter are controlled directly by the central processor and the data adapter timing is synchronous with that of the central processor timing. The primary data adapter functions are listed in Table 5.

The address generator decodes the nine operand address lines from the central processor upon receipt of a central processor PIO instruction. The decoded address selects the register, I/O processor memory location, or other circuitry in the data adapter that is to send data to or receive data from the central processor.

Addresses are divided into four basic groups as determined by the operand address bits A7 and A8. These groups are defined in Table 6.

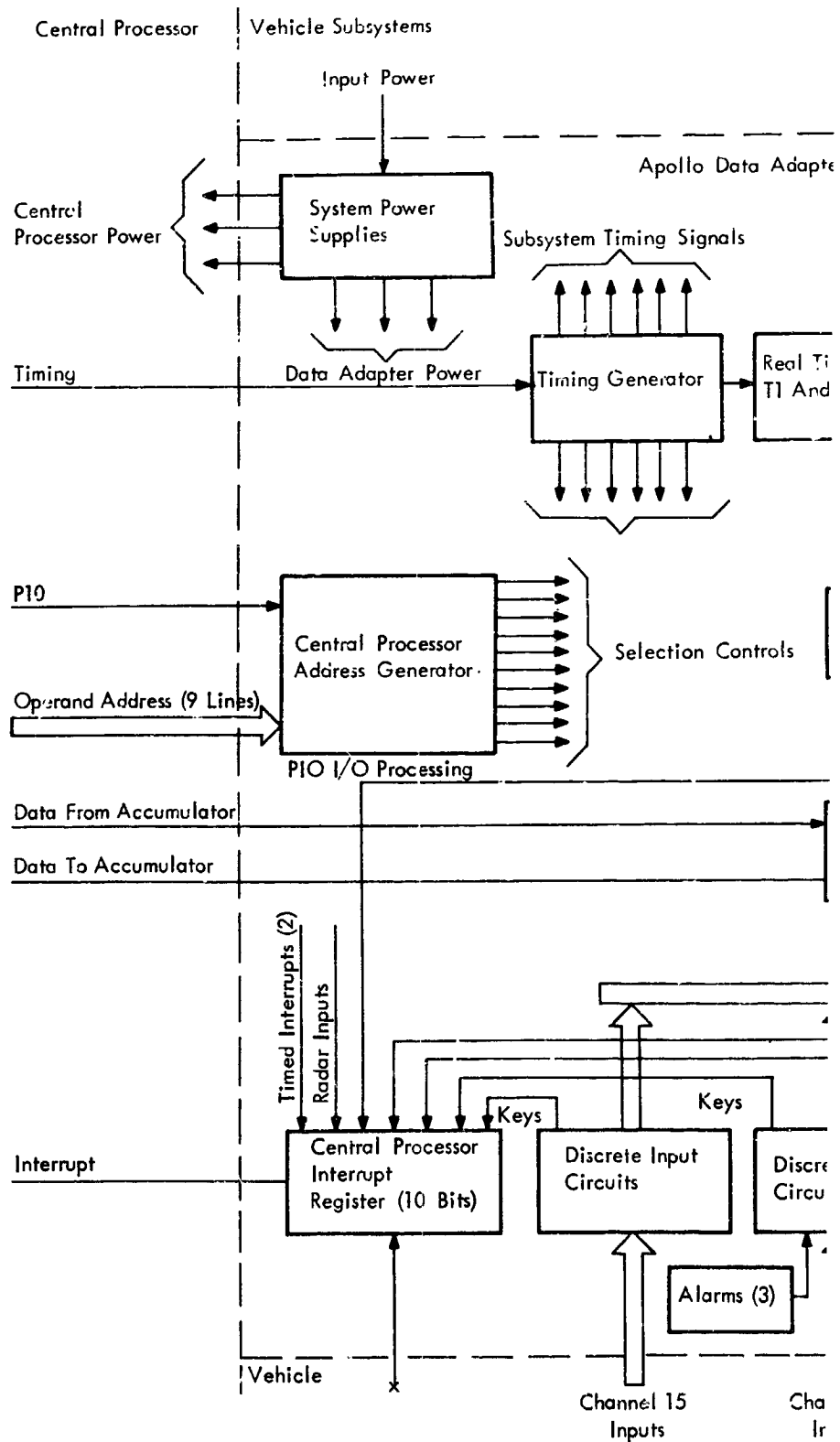
The data adapter contains a register addressed by the central processor for setting discretely which control internal functions. This register is designed so that the state of any output may be changed without momentarily or permanently affecting the state of any other unrelated outputs.

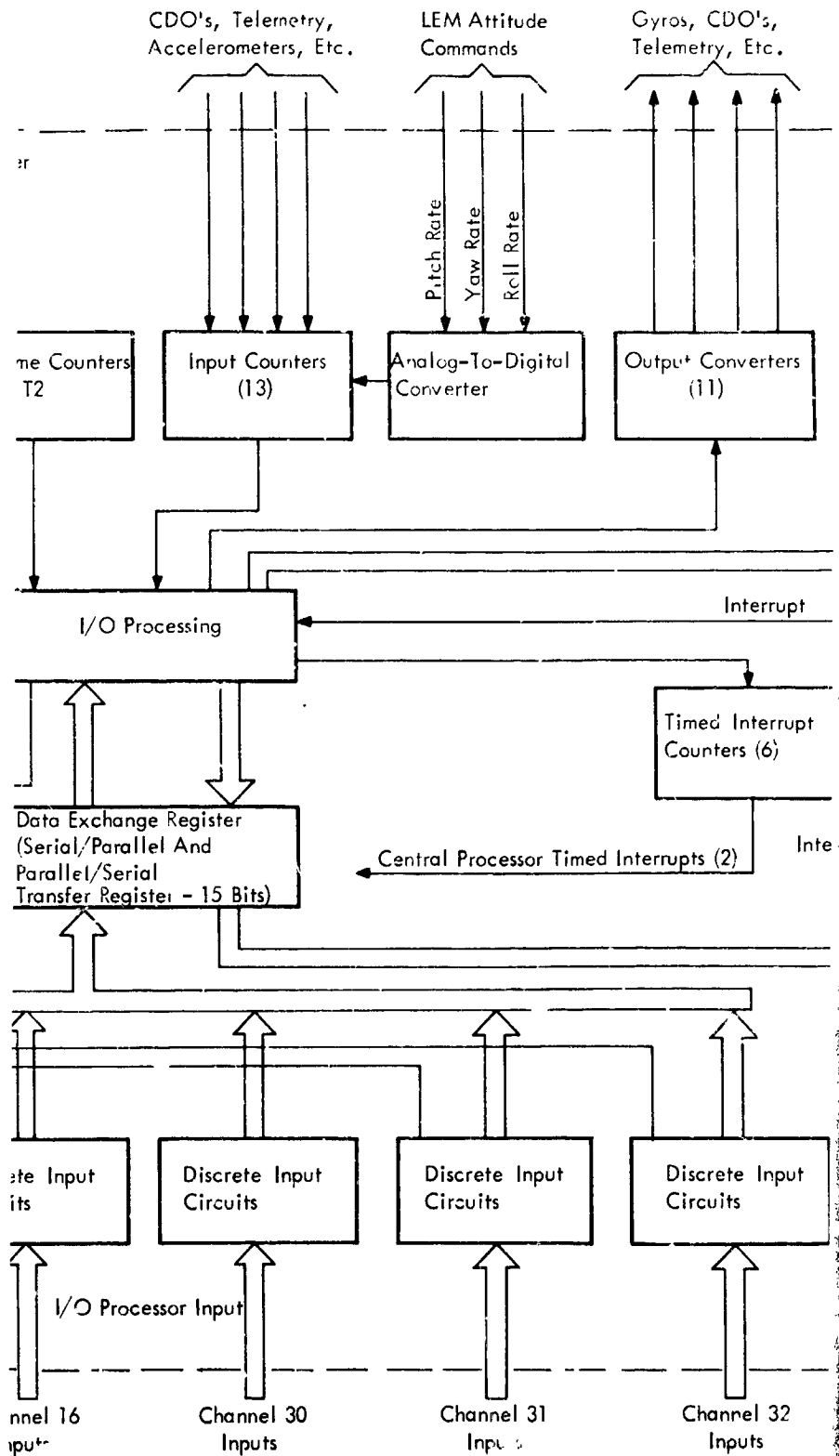
**TABLE 5 — Data Adapter Characteristics**

Item	Function	Description
Inputs	Discrete Pulsed	73 33 (Serial and Incremental)
Outputs	Discrete Variable Pulsed Fixed Pulsed	68 43 (Serial, Incremental, Discrete) 10
Modules	Output Counter	11 (Including Registers and Control), Gyro and Radar Counter Logic
	Input Counter	11 Counters, Multiplexer, Hand Control Logic, Boot Strap Loader
	Time Counter	9 Counters, Pulse Timing
	Data Flow	Data Exchange Register, Logic, Multiplexer
	Control	4 Discrete Output Registers, Address Decode, Controls
	Processor	Load Register, Down Link Register and Control, Interrupt Register
	Input/Output	Simplex Drivers

**TABLE 6 — Address Groups**

Group	A7	A8	Data Transfer Functions
1	1	0	Central processor accumulator to data adapter registers
2	0	0	Central processor accumulator to I/O processor memory
3	1	1	Data adapter inputs to central processor accumulator
4	0	1	I/O processor memory to central processor accumulator





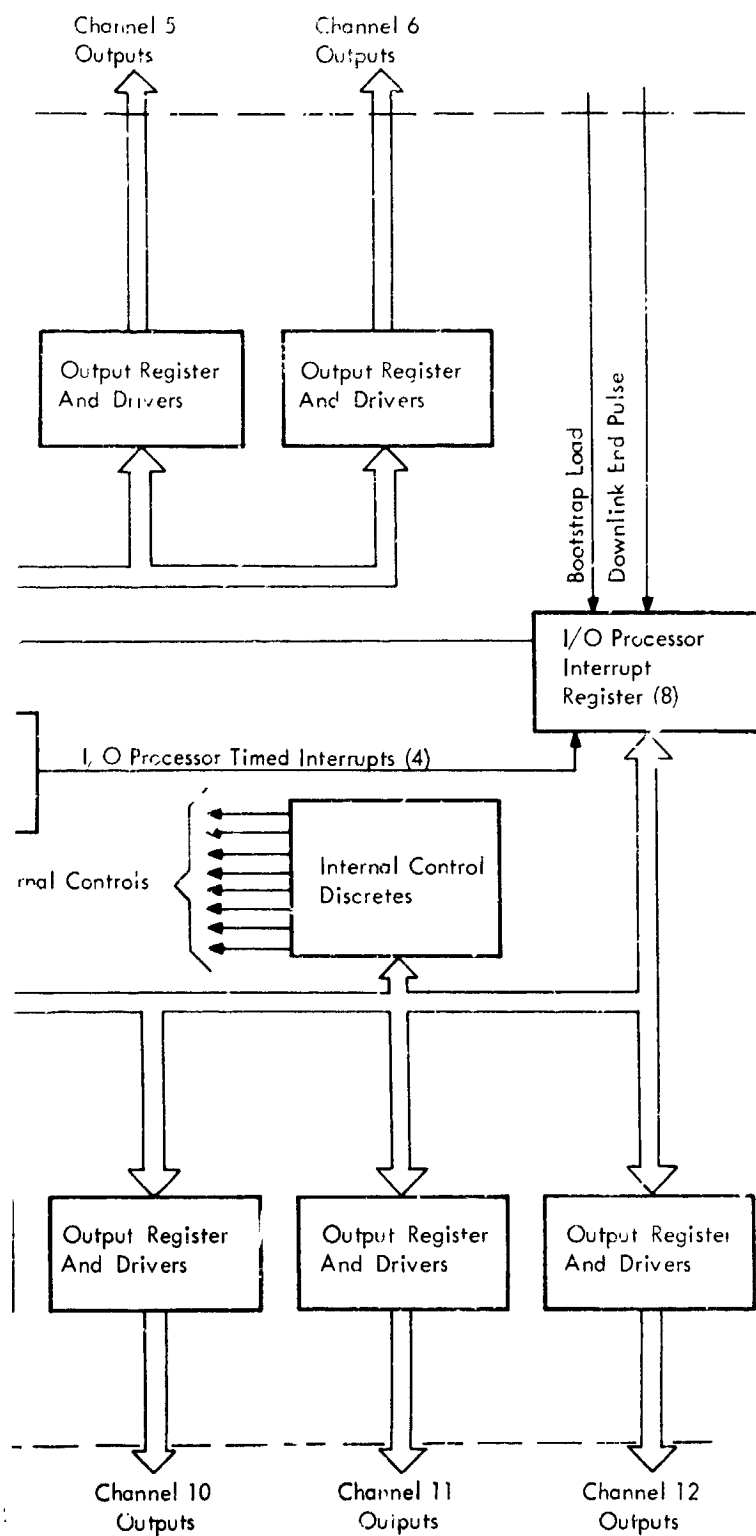


Figure 25. Data Adapter Block Diagram

The data adapter contains three output registers controlled by the central processor and ranging from 7 to 15 bits capacity. These registers are used to supply miscellaneous discrete signals to systems in the spacecraft and also for internal control within the data adapter. These registers are designed so that the state of any output may be changed under computer control without momentarily or permanently affecting the state of the other inputs.

To load a one in any bit position of one of these registers, the set address is used. The central processor data word must contain zeros in all bit positions except those to be set, which must contain ones. To load a zero in any bit position, the reset address must be used. The computer data word must contain zeros in all bit positions except those to be reset, which must contain ones.

The data adapter contains a 15-bit output register addressed by the central processor which is used to control display matrix relays in the display and keyboard (DSKY). At the start of each PIO load operation for this register, all bits are reset to the zero state automatically, allowing a new word to be loaded immediately thereafter.

The data adapter is capable of accepting 67 discrete inputs from spacecraft subsystems and four internally generated discrete signals. Except for the internally generated discretes, no storage is provided for discretes within the data adapter. Groups of these discretes are treated as words by the central processor. Each channel is addressed and read into the central processor by a PIO operation.

The data adapter contains a 10-bit register for storing signals required to interrupt the central processor. Some of these signals are generated internally; the others are caused by critical discrete inputs.

Upon receipt of one of these signals, it is stored in the register. Register outputs are "OR'ed" together so that any input signal will cause the central processor interrupt signal to be turned on. This signal will cause an interruption to occur when the instruction in process is completed.

At the start of an interrupt subroutine, the central processor will read the contents of the interrupt register. It will then process, in the order of highest assigned priority, any interrupt subroutines called for by the presence of ones in the interrupt word. Upon completion of an interrupt subroutine, the central processor will address the interrupt register and reset the register position causing the interrupt just

processed, as explained in the following paragraph. In the case of bit position 10 (switch closure) and keyboard inputs, further interrupts will not be recognized until the input stimulus has cycled down and back up after the original request. This prevents repeated processing of interrupt subroutines whose input signals last longer than the subroutines.

Certain interrupt sources may be inhibited or "trapped" under program control by the central processor. These are signals which would cause interrupts at undesired times during a mission if no protection against this were provided. To trap an interrupt, the Set Central Processor Interrupt Trap Address is used with a one in its related accumulator data bit position. Zeros are placed in the other positions of the data word. To remove the trap or to reset an interrupt register bit position after processing it, the Reset Central Processor Interrupt Trap Address is used. Accumulator data for untrapping or resetting is the same as for trapping.

The data adapter contains a 15-bit multipurpose shift register called the data exchange register (DER). This register performs the following functions:

- Accepts serial 512-kc/s data from the central processor accumulator and buffers and transfers it in parallel to the I/O processor memory drivers, the internal control register, or discrete output registers.
- Accepts parallel data from the I/O processor memory sense amplifiers, discrete input channels, or the central processor interrupt register and transfers it serially at 512 kc/s to the central processor accumulator.

The central processor accumulator data transferred to or from the DER is referenced to the sign and 14 high-order bit positions in the accumulator.

Some of the vehicle subsystems require timing signals from the Apollo backup computer. These signals are derived from the data adapter timing generator and are required continuously during all phases of the mission. Therefore, they must be available during the standby mode of operation.

Certain signals are continuously monitored for malfunctions. Upon detecting a malfunction, the computer system generates a discrete signal to turn on a warning light either on the DSKY or the caution

and warning electronics panel. Some of these signals are generated under program control; others are generated automatically by special alarm detection circuits.

The data adapter can accept and generate pulse train inputs and outputs for other spacecraft subsystems. It generates and stores the current value of real time required for navigation and control functions. It also generates program controlled, timed interrupt signals which are flags for branching into different subroutines. These functions are performed by counters and associated logic. Thirty-two counters are required.

There are 15 input counters serving various input functions. Input pulses occur at varying and unpredictable intervals in several of the channels and are therefore buffered, one pulse per channel, to await sampling in the processor, the buffer positions are continuously sampled consecutively at 1-clock pulse intervals to determine whether an input is present. A 5-bit grey code counter is used to step from input to input simultaneously with normal program cycles in the processor. Upon detecting an input pulse requiring storage, the grey code counter is stopped, and its value is transferred into the five low-order positions of the processor operand address register. The high-order bits are forced to zeros. This forms the memory address for that input counter. A memory-steal cycle is then executed incrementing or shifting the pulse into its memory location. The input buffer for that pulse is then reset to await the arrival of another input pulse.

There are 17 output counters serving various internal timing and output functions. When output pulses from any counter location are required, they occur at a fixed rate of 3200 pps. This means that a pulse occurs every 312 microseconds from the counter involved. It is convenient to service these counters using the same grey code address counter used for T8 and the input counters. For these latter counters, the grey code counter steps through 16 states and repeats. This operation is continuous except that every 312 microseconds an internally generated timing pulse occurs causing the address counter to extend its count from 16 to 32 to service the 16 other output counters. Each output counter has a buffer latch which is set or reset during the previous memory-steal cycle associated with the counter. It is also set by the central processor PIO operation used to initially load data in the output counter memory location. The added 16 counts from the address counter are used to sample the state of these buffer latches in the same manner as for the input pulses. The address counter also forms the memory address for memory-steal operations as described for the input counters. Any buffer latches that are set when addressed require

output pulses to be generated (one per channel per address pulse). When all 16 output counters have been sampled and processed as required, the address counter will again process the inputs repeatedly until interrupted by another 3200-pps pulse. This operation is repeated every 312 microseconds until the counter memory locations have been cleared, thus freeing them for loading more output data.

The downlink implementation provides for transmitting a one bit identifier (word order bit) followed by 32 information bits. This information group will be two 15-bit accumulator words, each followed by a separate parity bit.

The downlink output is controlled by the number of synchronization pulses received from the pulse code modulator (PCM) telemetry and the manner in which the processor is programmed. Therefore, the output can be one word, one word redundant, or two words, depending upon how the downlink registers are loaded and the number of data synchronization pulses gated into the data adapter. If only one word is sent out, the second load PIO operation is still required to advance the output data from the load register to the shift register. This PIO word will contain all zeros.

The downlink operation sequence is initiated by an input pulse (downlink end) which causes a processor program interrupt. During the interrupt subroutine, the processor performs a PIO operation to set the downlink word order bit to a one or zero as required. The processor then loads the first downlink word, which goes into the load register. This operation is followed by another PIO to transfer the first downlink word to the shift register and load the second downlink word, if required, into the load register. This completes the processor interrupt subroutine: The data remains in storage registers until the pulse coded modulation (PCM) telemetry sends the next series of control and synchronization pulses required to send the data to the PCM equipment. When the first 15-bit word has been transferred out of the shift register, a five-stage counter in the downlink timing and control logic causes a parity bit to be generated for that word. It also causes the second data word to be transferred from the load register to the shift register. When this second word has been transferred to the PCM telemetry, its parity bit is also generated and sent out.

There are two downlink data word transfer rates: 51.2 kpps and 1.6 kpps. The rate used is determined by the rate of the synchronization pulses received from the PCM equipment.

The data adapter contains the system power supplies. These supplies furnish normal power for the central processor and data adapter and standby mode power when normal computer operations are not required. Input power to the supplies is obtained from duplex redundant 28-volts dc vehicle power sources. Power sequencing and input power transient protection are provided to prevent loss of data stored in the central processor memories.

In certain phases of the mission there may be relatively long periods when it will not be necessary for the Apollo computer to perform any calculations. The only use for the computer during these periods is to keep track of real time and provide continuous timing signals for other vehicle subsystems. Since these are only minor functions, a standby power supply is provided to furnish power only for the logic associated with these functions.

During standby operation the oscillator and clock logic of the central processor is used to drive a group of clock drivers which are associated only with the standby logic.

Real time is derived from the pulse timing logic, the lowest frequency of which is 800 cps. This 800-cps signal is used as an input to counter T2. The overflow of this counter is used to increment counter T1. The two counters form the low and high-order bits of real time, respectively. It is, therefore, possible to record time to  $(1.25 \times 10^{-3})$  ( $2^{30}$ ) seconds or approximately 15 1/2 days.

Time recording during standby requires the operation of the pulse timing logic, counter T1, counter T2, add/subtract logic, and processor memory. Memory must operate because the contents of counters T1 and T2 are stored in memory locations.

Standby power is established by request of the operator. An interlock system was designed to prevent the operator from inadvertently requesting the standby mode. The first step required to initiate standby is to insert the proper key code. When the central processor recognizes this code, it prepares itself and the discrete outputs for shutdown. After this is completed, the central processor sets the discrete output in channel 13, bit 10. This signal is an enable signal which energizes the standby switch on the DSKY. Depressing the standby switch in conjunction with the enable signal causes the power supply to start turning off main power.

### 2.3.3 Reliability Models

A reliability model for the basic computer subsystem consisting of the Saturn-V computer and a redundant version of the Apollo backup data adapter was derived and used as a basic reference with which to compare the reliability characteristics of the reorganized computer and data adapter.

The model includes "equivalent time" factors which modify real time to include the effects of environmental severity factors and non-operating failure rates. The equivalent time period of the most critical mission phase is defined as:

$$T_c = \max_{i=1}^m (T_i K_i)$$

where  $T_i$  is the actual time period of the  $i^{\text{th}}$  phase,  $m$  is the number of critical mission phases, and  $K_i$  is the environmental severity factor for the  $i^{\text{th}}$  phase. The simplex reliability model for the most critical mission phase is defined as

$$R_c = \exp(-\lambda_{op} T_c),$$

where  $\lambda_{op}$  is the operating failure rate of the equipment. The equivalent operating time and standby time is generated for each of the three assumed duty cycles from the expressions

$$T_{E_{op}} = \sum_{i=1}^n T_{op\ i} K_i$$

$$T_{E_{non-op}} = \sum_{i=1}^n T_{non-op\ i} K_i$$

where  $T_{E_{op}}$  is the equivalent mission operating time,  $T_{E_{non-op}}$  is the equivalent mission standby time,  $T_{op\ i}$  and  $T_{non-op\ i}$  are the actual operating and standby times,  $K_i$  is the environmental severity factor for the  $i^{\text{th}}$  phase, and  $n$  is the number of mission phases. The simplex reliability model for the total mission is defined as:

$$R_m = \exp(-\lambda_{op} T_{E_{op}} + \lambda_{non-op} T_{E_{non-op}}),$$

$\lambda_{non-op}$  is the standby failure rate of the equipment.

The computer and data adapter operate effectively in series for reliability computations so the model for the computer subsystem is simply

$$R_{ss} = R_{co} R_{da},$$

where  $R_{co}$  is the computer reliability and  $R_{da}$  is the data adapter reliability.

The computer is composed of a simplex oscillator, TMR logic, and duplex memories. These three elements operate effectively in series so the reliability model for the computer is

$$R_{co} = R_{osc} R_{log} R_{mem}.$$

The oscillator for the Saturn-V computer is simplex so the reliability model for this device is

$$R_{osc} = e^{-\lambda_{osc} T}.$$

The reliability of the computer logic (including timing) can be expressed mathematically as

$$R_{log} = (R_{tg})^3 (R_{TMR}) + 3 (R_{tg})^2 (1 - R_{tg}) (R_{sim})^2,$$

where  $R_{tg}$  is the reliability of the simplex timing generator,  $R_{TMR}$  is the reliability of the TMR logic, and  $R_{sim}$  is the reliability of one channel of the TMR logic. The reliability model for the TMR logic was defined as

$$R_{trio} = 3 (R_{mod})^2 - 2 (R_{mod})^3,$$

where  $R_{mod}$  is the reliability of each simplex module of a TMR module trio. For  $p$  independent trios

$$R_{TMR} = \prod_{i=1}^p (R_{trio})^i.$$

The reliability of the duplex memory is represented by the model

$$R_{\text{mem}} = (R_{\text{sm}})^2,$$

where  $R_{\text{sm}}$  is the reliability of each of the simplex memories. The reliability of a simplex memory can be expressed mathematically as

$$R_{\text{sm}} = R_M + P_{\text{ND}} \cdot P_p (1 - R_M) R_M + P_D (1 - R_M) R_M,$$

where  $R_M$  is the probability that the originally selected simplex memory works for the entire mission,  $P_{\text{ND}}$  is the probability that a failure in the selected memory will not be detected by the error sensing circuitry,  $P_p$  is the probability that these nondetected errors will be detected by parity, and  $P_D$  is the probability that a failure in the selected memory will be detected by the error sensing circuitry.

The data adapter is composed primarily of the power supply and the logic, and the reliability model is the serial combination

$$R_{\text{da}} = R_{\text{ps}} R_{\text{dal}},$$

where  $R_{\text{ps}}$  is the reliability of the power supply and  $R_{\text{dal}}$  is the reliability of the data adapter logic. The power supply model assumed for the AES configuration is based on the Saturn-V duplex power supply which is composed of six individual duplex supplies using duplex error amplifiers. The reliability model for the AES power supply system is then

$$R_{\text{ps}} = \prod_{i=1}^p R_{\text{di}},$$

where  $R_{\text{di}}$  is the reliability of the  $i$ th duplex supply.  $R_d$  can be expressed mathematically as

$$R_d = R_s^2 R_I^2 + 2 R_s^2 R_I (1 - R_I) + 2 R_s R_I P_{\text{sf}} (R_I + P_{\text{if}}),$$

where  $R_s$  is the reliability of a simplex supply with duplex error amplifier,  $R_I$  is the reliability of a simplex isolation circuit,  $P_{\text{sf}}$  is the

probability that the simplex supply will fail low,  $P_{ifl}$  is the probability that the isolation circuit will fail low. The reliability of the simplex supply is

$$R_s = R_c R_a^2 + 2 R_c R_a P_{afl},$$

where  $R_c$  is the reliability of the simplex DC/DC converter,  $R_a$  is the simplex reliability of the duplex error amplifiers,  $P_{afl}$  is the probability that an error amplifier will fail low. For supplies not containing an isolation circuit

$$R_d = R_s^2 + 2 R_s P_{sfl}.$$

The simplex Apollo data adapter may be arranged into  $p$  functional modules and each of these assumed to be TMR for the AES configuration. The reliability of each TMR module is, as in the case of the computer TMR logic,

$$R_{trio} = 3 (R_{mod})^2 - 2 (R_{mod})^3$$

and the reliability of the data adapter logic is

$$R_{dal} = \prod_{i=1}^p (R_{trio})_i.$$

#### 2.3.4 Reliability Estimates

Simulations were performed to derive reliability estimates for the basic subsystem configuration based on the reliability models of the previous section and using the component failure rates, environmental stress factors and mission profile.

The reliability estimates are summarized in Table 7 for the most critical phase and mission reliabilities. The latter was estimated for duty cycles of 100, 50, and 25 percent and for zero and nonzero standby failure rates. The mission reliability figure represents the basic long-term reliability of the equipment with no sparing. The sparing requirements to raise these figures to the required 0.9994 mission reliability were not determined for the basic system because the predicted system reliability for the most critical phase (0.999921) fell

below the system requirement of 0.999999. Although memory appeared to be the limiting factor, the TMR memories proposed for the reconfigured computer provide higher reliabilities and the TMR/simplex mode further improves both memory and logic reliabilities. However, since the reliability estimate for the simplex oscillator was less than the required system reliability, a redundant oscillator was a necessary component of the reconfigured computer. Also, two of the six regulators in the Saturn-V power supply did not contain isolation circuits, which resulted in considerably lower reliability than the four regulators containing this protection. Addition of isolation to these circuits was considered in the reconfigured supplies as well as triplex instrumentation. TMR memory and module switching was also considered in the reorganized computer system to increase the inherent equipment reliability to the specified 0.999999.

## 2.4 Oscillator

The reliability estimate for the basic computer given in Section 2.3 revealed that the simplex Saturn-V oscillator presented a reliability constraint which will prevent any reconfigured computer from meeting the short term requirement of 0.999999 specified in the AES-EPO statement of work. A redundant oscillator investigation was therefore performed during August to find a technique for providing a redundant oscillator and thereby removing this reliability constraint.

### 2.4.1 Alternate Approaches

A previous IBM oscillator study considered two general approaches to oscillator design for space system applications: 1) an astable multivibrator (saturated stages) and 2) a sine wave oscillator (outputs shaped into symmetrical square waves). The second technique could be accomplished with tuned circuits, consisting of normal inductors or capacitors, or with piezo-electric crystals.

The astable multivibrator was eliminated from consideration for the AES computer for several reasons including frequency, accuracy, stability, and temperature sensitivity. Redundancy and crystal control are feasible in the multivibrator pulse generator, but the required pulse characteristics could not be maintained in the presence of a fault even though the pulse repetition frequency might be maintained.

Conventional sine wave oscillators were eliminated from consideration mainly because of the high component count in redundant

TABLE 7 — Reliability Estimates (Basic System)

Element	Critical Phase	Mission Reliability				
		100%	Non-Op $\lambda > 0$		Non-Op $\lambda = 0$	
			50%	25%	50%	25%
Computer	0.999933	0.8879	0.9272	0.9446	0.9647	0.9886
Oscillator	0.999992	0.9984	0.9989	0.9992	0.9992	0.9996
Logic	0.999998	0.9334	0.9580	0.9686	0.9809	0.9947
Memory	0.999942	0.9528	0.9689	0.9760	0.9843	0.9943
Data Adapter	0.999989	0.8096	0.8921	0.9272	0.9429	0.9840
Power Supply	0.999995	0.9980	0.9988	0.9992	0.9992	0.9997
Logic	0.999994	0.8113	0.8932	0.9280	0.9436	0.9843
Computer Subsystem	0.999921	0.7189	0.8272	0.8759	0.9096	0.9728

configurations, especially TMR. The poor frequency accuracy and stability inherent to non-crystal sine wave oscillators, and the required adjustments, were additional reasons for their elimination, although precise frequency is not necessarily a systems requirement for computer timing if delay lines are not used and if real time is derived from a separate source.

A special crystal-controlled oscillator was chosen for the AES computer in preference to crystal stabilized instrumentations to provide a precise timing source with a minimum component count and no required adjustments. Several redundant configurations of this basic crystal controlled oscillator were considered.

The maximum reliability increases are achieved generally when redundancy is applied to the lowest circuit levels. Quad circuits apply redundancy at the component level by arranging sets of four identical components in series, parallel, or series-parallel. Five different

quad circuit configurations of the crystal oscillator were considered for the AES computer and rejected for the following reasons:

- 1) Excessive component count.
- 2) Quad crystal circuits tend to cause heterodyning of the output frequency, especially in the presence of a component failure, except in the configuration in which the four crystals were connected directly in parallel.
- 3) Certain failures such as shorts at the junctions of transistors will cause system failure, a violation of the design ground rule that single component failures shall not cause failure of the redundant system.
- 4) Output wave shapes changed in unacceptable manners when a component failure occurred in all but one of the five configurations studied.
- 5) A transient occurred in the output of the redundant oscillator when a component failure occurred.

A redundant oscillator configuration was considered in which two independent oscillators are operated in parallel but synchronized by appropriate coupling. Inductive coupling was rejected because the inductor becomes a significant factor in the equivalent crystal circuit and therefore detracts from the desired crystal control. Resistive coupling was rejected because shorted transistor junctions will cause system failure. Capacitive coupling is feasible but requires more components, dissipates more power, and yields lower reliability than the DC-AC-DC synchronized crystal controlled oscillator described next.

This oscillator, a duo redundant configuration developed for the OAO system, uses a pair of piezo-electric crystals as couplers as well as resonators. The crystals couple the driving currents into the basis of the transistors. The primary disadvantage of this scheme is the occurrence of a component failure. The reliability estimate of this redundant oscillator for the critical phase of the AES mission exceeds 0.9999999.

#### 2.4.2 Synchronization and Transients

Two problems must be solved in instrumenting a TMR oscillator:  
1) synchronization of the three oscillators and 2) elimination of the

transient which will appear at the voter outputs when a component failure occurs in one of the oscillators.

Synchronization can be obtained by slaving the oscillators as shown in Figure 26. The channel 1 oscillator may be considered the master oscillator; it drives the channel 2 oscillator, which in turn drives the channel 3 oscillator. As long as the channel 1 oscillator is operating, channels 2 and 3 will be slaved to channel 1. If channel 1 fails, however, the channel 2 oscillator becomes the master and forces channel 3 to synchronize with it.

Elimination of the loading transient can be obtained by inserting time delays in the three channels between the oscillator buffers and the voters. The delay in each channel will be different by an amount at least equal to the period of the loading transient (which should not exceed one cycle, although much larger transient periods could be accommodated). The relative delays between channels must also be an integral number of oscillator output periods. The outputs of the delay circuits and of the voters are shown in Figure 27. Note that the transient (assume to be a failure in channel 1 oscillator) is voted out.

Analysis of the Saturn-V timing indicated, further, that neither the delay nor the synchronizing may be necessary. A functional representation of the Saturn-V clock generator is shown in Figure 28. The generator is shown in simplex for simplicity. The generation of the clock pulses is sequential (w derived from z, x from w, y from x, and z from y). The beginning of each clock (say x) is determined from the

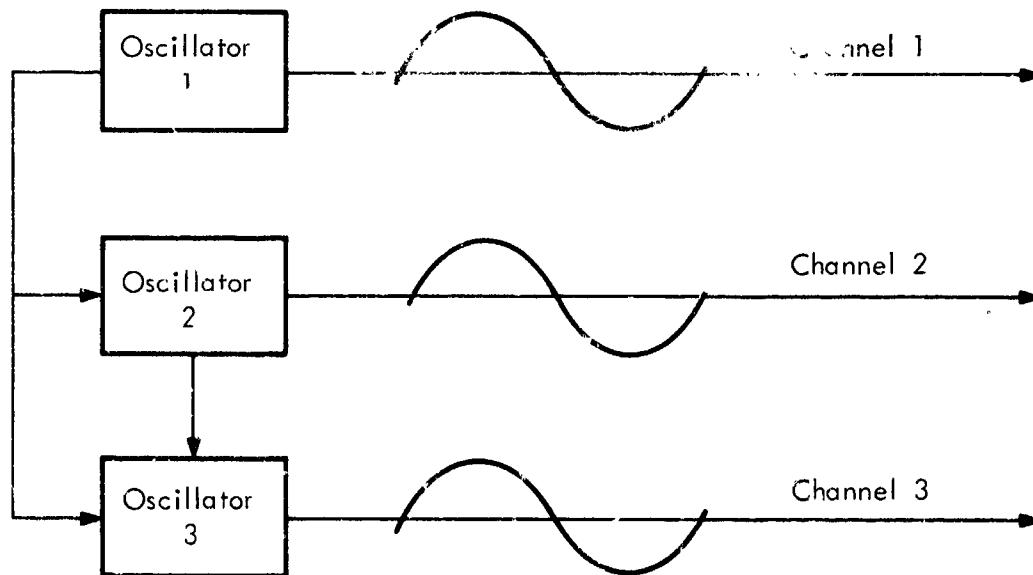


Figure 26. Oscillator Synchronization

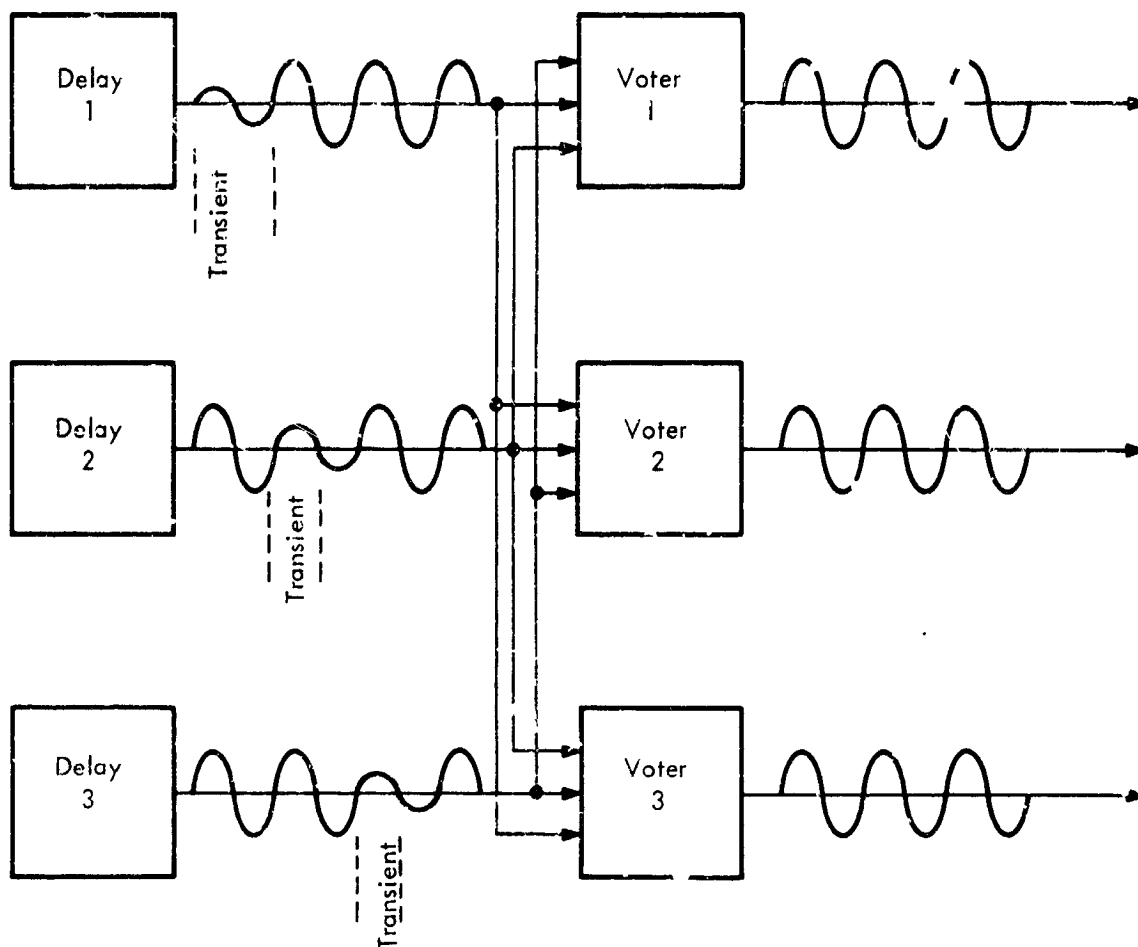


Figure 27. Transient Filter

change in state of the preceding clock ( $w$ ) in the direction of reset (on to off). Normal operation is indicated in Figure 28 by the solid-line waveforms.

If the oscillator fails by missing a pulse, indicated in Figure 28 by the dotted-line waveforms, the only result is an elongation of one of the clock pulses. In Figure 28, the second oscillator pulse is missing which delays reset of the  $w$  clock for one oscillator period. The remaining clocks are undistorted but delayed by the transient period.

Operationally, the effect of the elongated clock pulse is effectively a suspension in computation for the period of the transient providing that the computer does not contain fixed-time components such as delay lines and provided that the transient is not so long that it affects the accuracy of real-time computations. The computer configuration

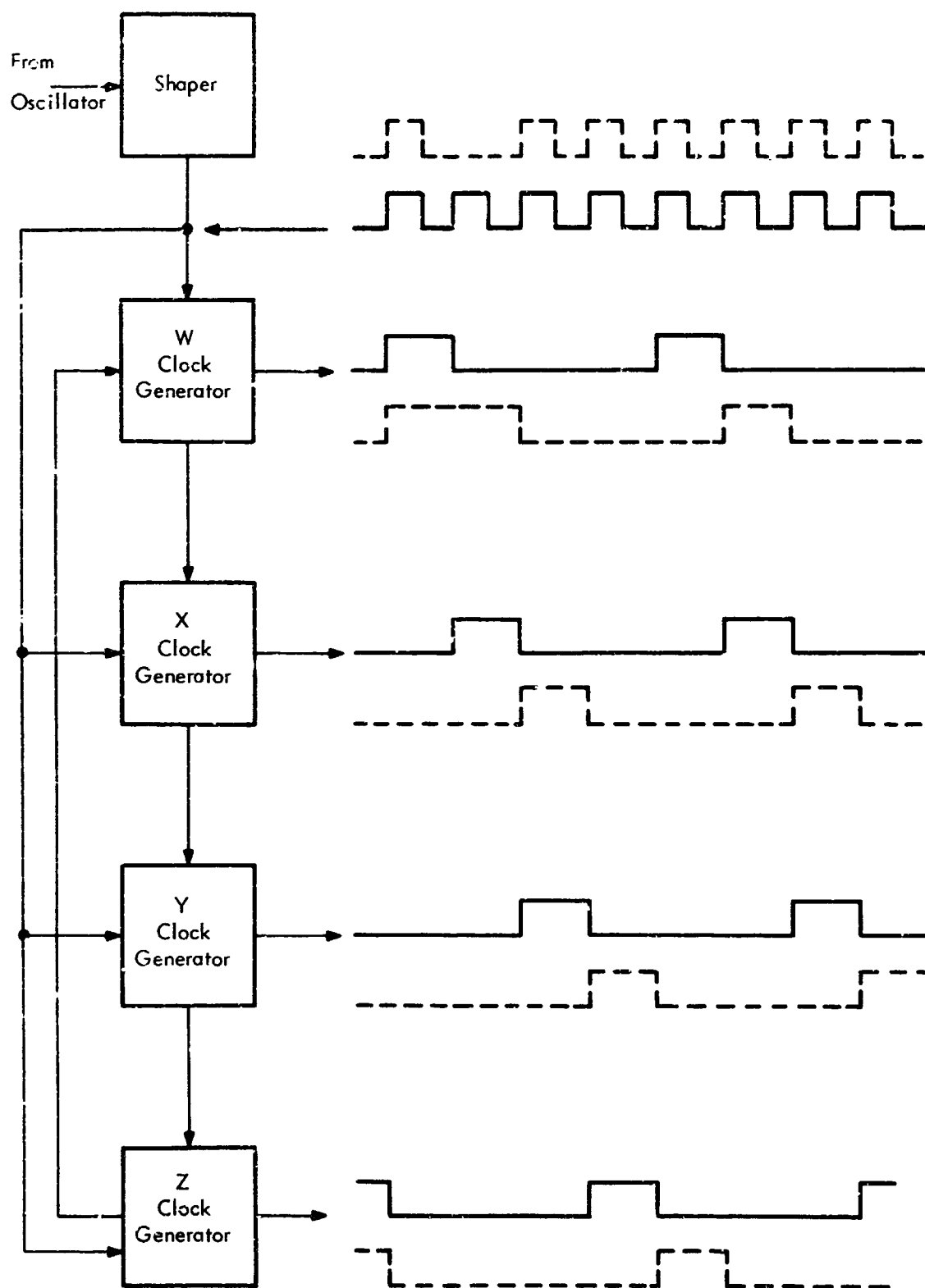


Figure 28. Clock Generator

visualized at this time for the AES application does not contain delay lines, and experience at IBM indicates that the transient period will be of a short enough period that real-time accuracy will not be affected.

Loading transients caused by oscillator component failures could conceivably result in double oscillator pulses rather than missing pulses. The bandwidth of properly designed clock circuits would not respond to a double pulse (double frequency), however, and the effect would be the same as a missing pulse. Similarly, if a distorted pulse occurred, rather than a missing or a double pulse, then the result would be a normal clock output (if the clock circuits responded to the distorted waveform) or a delayed clock output (if the clock circuits did not respond).

The conclusion of the preceding discussion is that the delay circuits described previously may not be necessary. In addition, frequency synchronization of the redundant oscillator may not be necessary as indicated by the following discussion.

#### 2.4.3 Selected Approaches

In addition to the TMR oscillator, two other redundant oscillator configurations were considered to be feasible. One scheme is shown in Figure 29 in which the outputs of three oscillators are tied together and the common output used to drive all three channels of the TMR machine. Each oscillator develops a d-c voltage (in addition to the sine

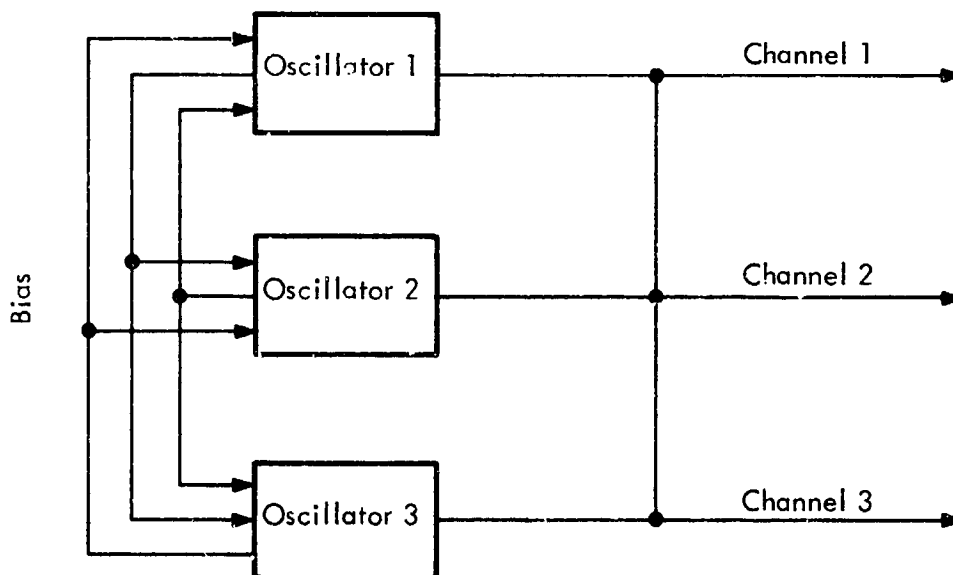


Figure 29. Biased Oscillators

wave output) to bias the other two oscillators off. When the power is first applied, all three oscillators try to build-up oscillations but one will win the race and turn the other two off. This winner will supply the basic timing for the entire TMR computer unless it fails, at which time the remaining two oscillators race for control.

A transient will occur upon occurrence of a component failure in the operating oscillator due to the time it takes the second oscillator to build-up to a usable output. Again this transient will cause only a clock elongation which effectively halts computation for the length of the transient. In this scheme, however, the transient can be of the order of a millisecond rather than an oscillator cycle, and a serious error may result, especially in the computation of real-time.

A possible solution to this problem is to develop real time from an independent simplex oscillator. To provide sufficient reliability for real-time computations, the triplex oscillator of Figure 29 may provide backup for real time computation, i.e., the triplex oscillator may be automatically switched to update the real-time counter when a malfunction is sensed in the simplex oscillator.

A third scheme of redundancy of the oscillator is to allow three independent oscillators to operate in parallel and gate their outputs so that only one is used at a time as shown in Figure 30. The output of each oscillator is checked by the sense circuits to verify operation of that channel. The latch and sequence circuits select an operating channel and provide a gating signal (say UO1, use oscillator 1) to the selected channel gate. The gate outputs are tied together to drive the TMR channels.

This scheme reduces the transient time to that required for switching (since all three oscillators are operating) and should be of the order of microseconds.

All three schemes (TMR, biased, and gated oscillators) appear to be feasible for use in the AES computer. The gated oscillator scheme was selected as the reliability and performance model for the reorganized subsystem.

## 2.5 Memory

The reliability estimate for the basic computer given in Section 2.3 revealed that the duplex Saturn-V memories, like the simplex oscillator, presented a reliability constraint which precludes the

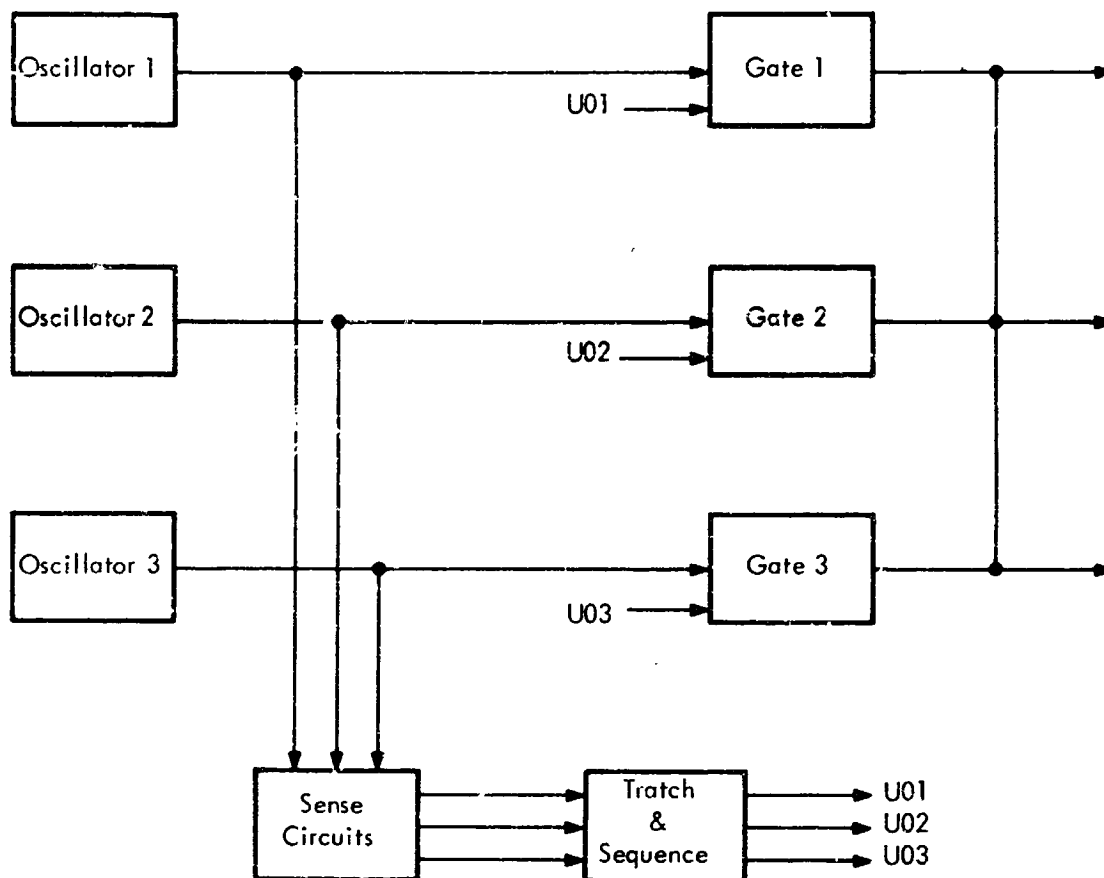


Figure 30. Gated Oscillators

short-term AES reliability requirement of 0.999999. A reorganization of the computer memory from duplex to TMR was found to provide increased reliability in this critical area as well as a potential for improved transient protection. Although the total memory capacity was increased 50 percent over the equivalent duplex configuration, much of the circuitry associated with duplex memory was eliminated including:

- 1) Half-select current monitoring circuits
- 2) Parity generating and measuring circuits
- 3) Buffer registers and associated switching
- 4) Voters on X-Y drivers
- 5) Voters on R-W timing.

The functional block diagram of the duplex memory of Saturn V and the TMR memory of the proposed AES configuration are shown in Figures 31 and 32, respectively.

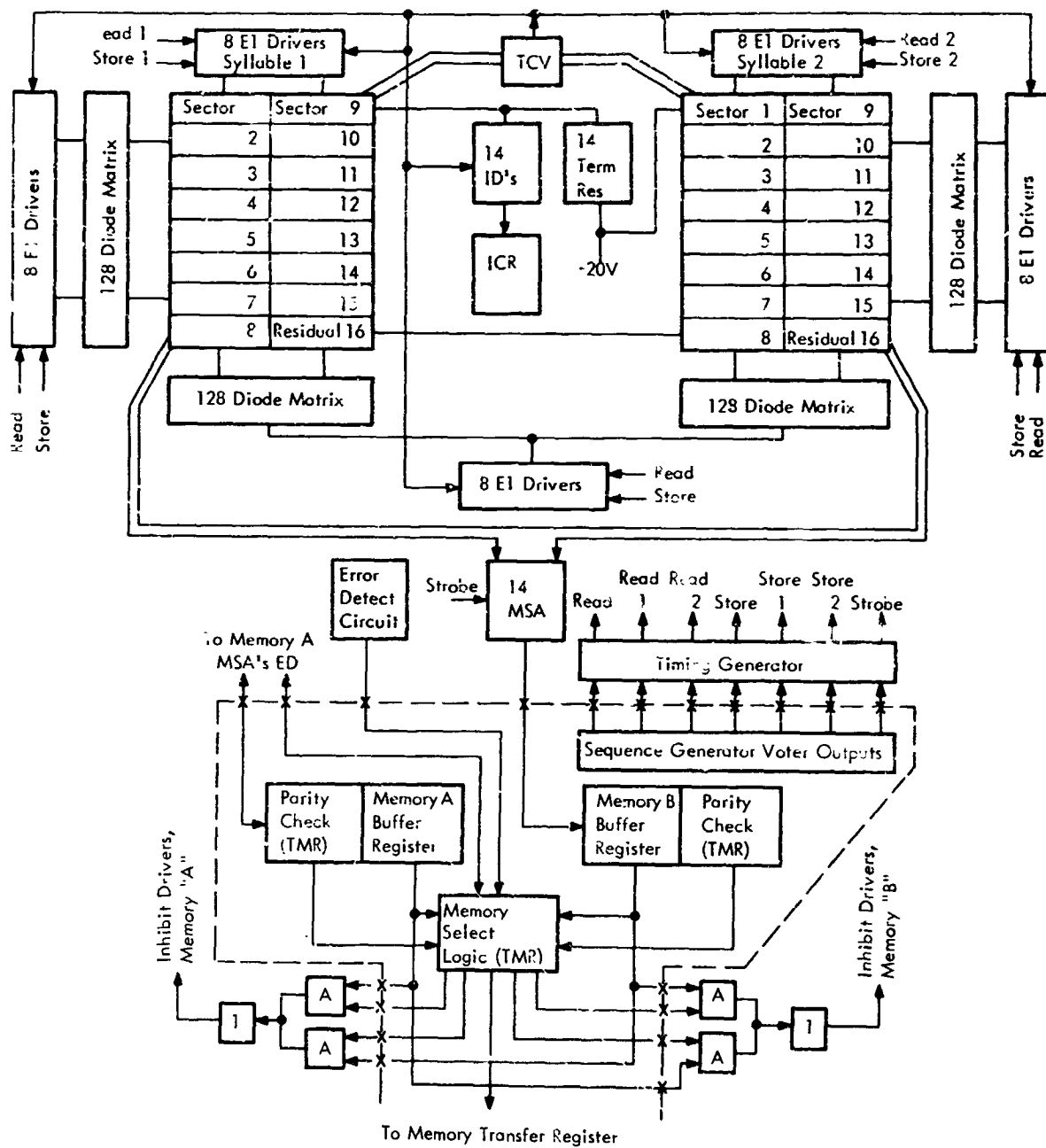
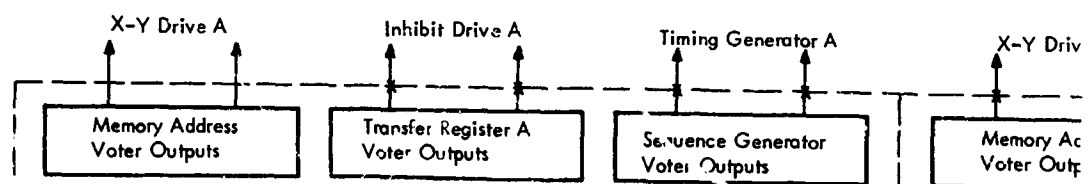
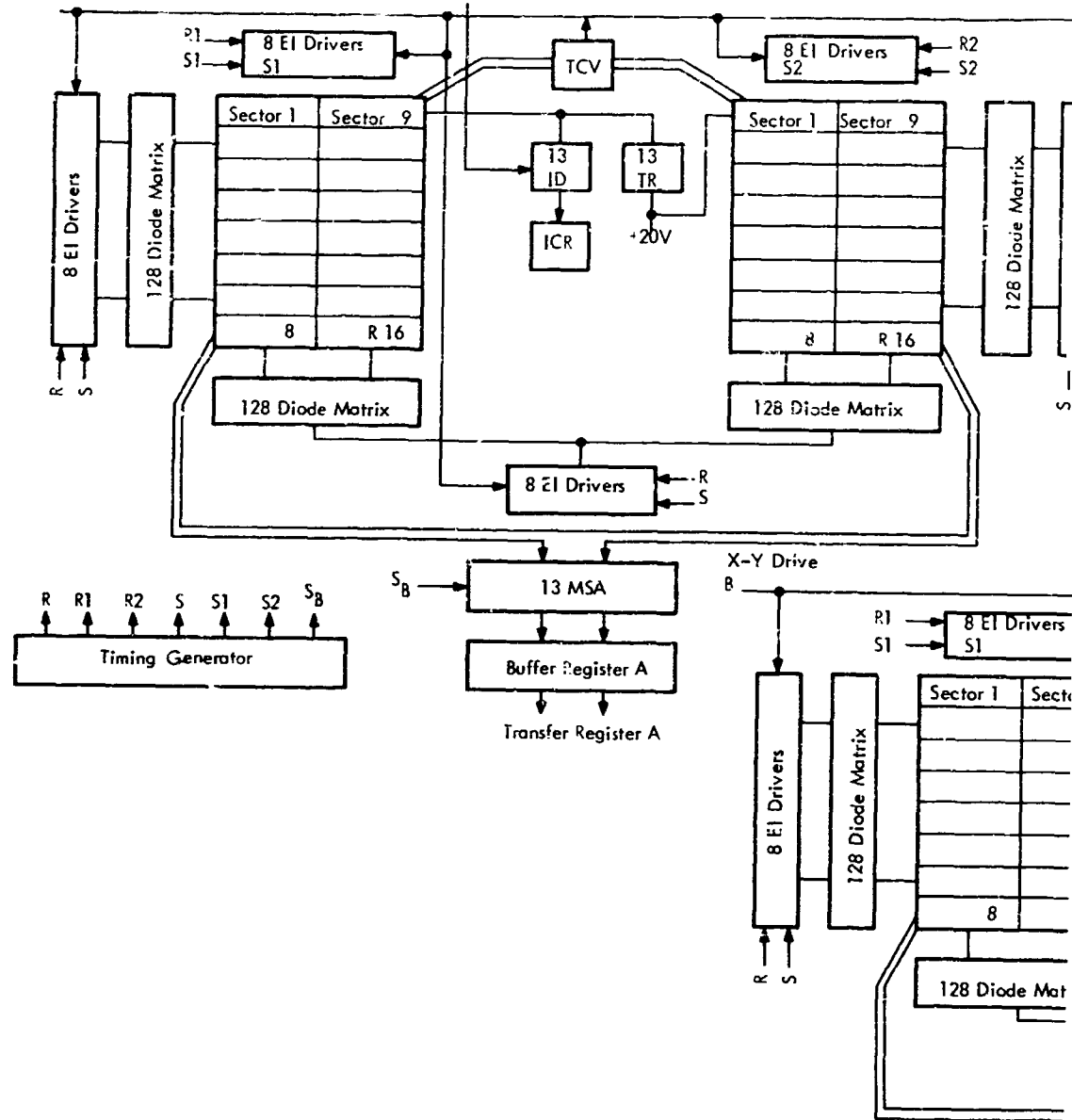
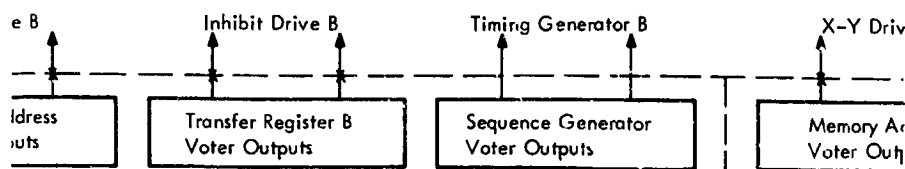
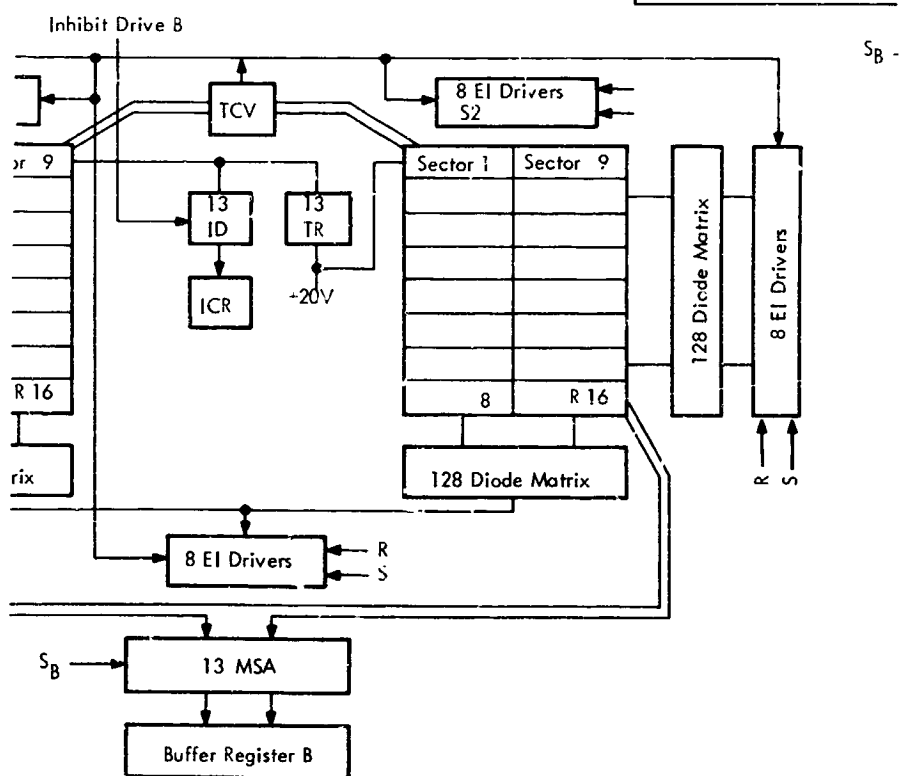
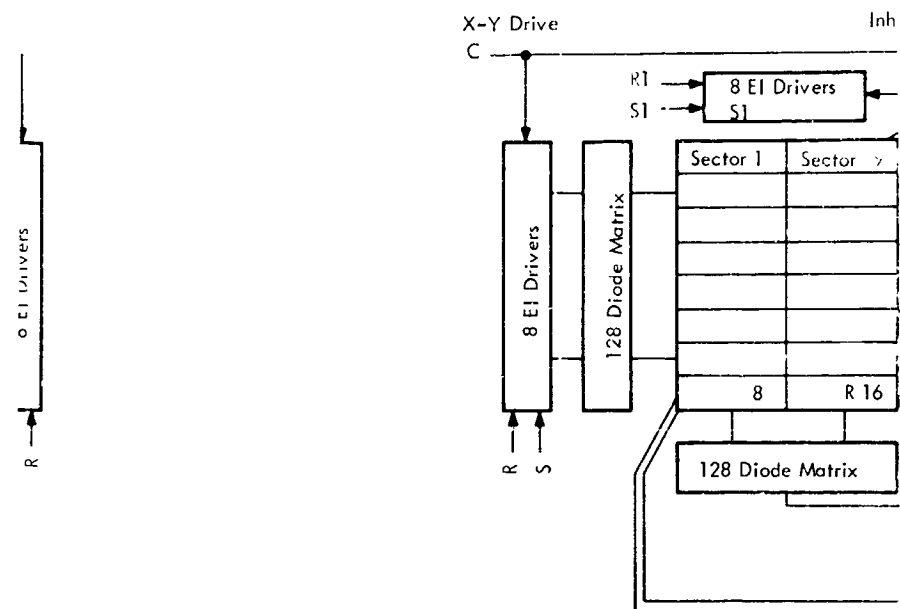


Figure 31. Duplex Memory

X-Y Drive A

Inhibit Drive A







### 2.5.1 TMR Reliability Model

A reliability analysis of a TMR memory configuration was performed and compared with the duplex configuration of the basic computer. Reliability of the TMR memory may be expressed in the following form:

$$R_{\text{TMR}} = R_M^3 + 3 R_M^2 (1 - R_M) + C_{s2} (3 R_M) (1 - R_M)^2 + C_{s3} (1 - R_M)^3$$

where  $R_M$  is the reliability of one simplex memory module of the trio,  $C_{s2}$  is the conditional probability that no identical address bit has failed in the two failed modules, and  $C_{s3}$  is the conditional probability that no identical address bit has failed in the three failed memory modules. This expression is conservative in that it does not recognize the possibility of compensating errors.

The failure events included in the  $(1 - R_M)$  probability expression consist of one, two, etc., component part failures and will have a conditional distribution of

$$(C_1 + C_2 + \dots + C_n) = 1.0,$$

where  $C_i$  is the conditional probability that  $i$  component part failures have occurred in a given module failure. Since the number of components in each memory is large and the probability of failure associated with each component is small, a Poisson distribution can be assumed in evaluating  $C_{s2}$  and  $C_{s3}$ . Therefore,

$$C_i = \frac{e^{-\lambda_m T} (\lambda_m T)^i}{i! (1 - e^{-\lambda_m T})},$$

where  $T$  is the equivalent time (real time times environmental stress factor) of the most critical mission phase and  $\lambda_M$  is the failure rate of a simplex memory module.  $C_{s2}$  and  $C_{s3}$  can then be expressed as

$$C_{s2} = \sum_{j=1}^n \sum_{i=1}^n C_j C_i K_{ji}$$

$$C_{s3} = \sum_{j=1}^n \sum_{i=1}^n \sum_{k=1}^n C_j C_i C_k K_{jik},$$

where  $K_{ji}$  is the conditional probability that no identical address bit failure has occurred, given  $j$  component failures in one memory module and  $i$  failures in a second module.  $K_{jik}$  is the conditional probability that no identical address bit failure has occurred, given  $j$  component failures in one memory module,  $i$  failures in a second module, and  $k$  failures in the third module.

$C_{s2}$  and  $C_{s3}$  were evaluated on the basis of no more than two component failures in each memory module, since the resulting unevaluated events are negligible. In order to determine  $K_{ji}$  and  $K_{jik}$ , the memory module component part failures were categorized as

- 1) Serial failures (failure results in complete memory module failure, i.e., all bits failed)
- 2) Core failures
- 3) High X driver failures
- 4) Low X driver failures
- 5) High Y driver failures
- 6) Low Y driver failures
- 7) Z failures (memory buffer register, sense amplifiers, inhibit drivers)
- 8) Y line failures (including Y line solder connections, terminating resistors and open failure mode of the decoupling diodes)
- 9) X line failures.

The value of  $(1-K_{11})$  was determined from an analysis of 81 categorized failure combinations. Since no more than two component part failures are assumed, the expected distribution of the second component part failures was assumed to be the same as for the first, or

$$\begin{aligned}
1 - K_{12} &= (1 - K_{11}) + K_{11} (1 - K_{11}) \\
&= 1 - K_{11}^2 \\
K_{12} &= K_{21} = K_{11}^2.
\end{aligned}$$

Similarly,

$$\begin{aligned}
K_{22} &= K_{11}^4, \\
K_{111} &= K_{11}^3, \\
K_{112} &= K_{121} = K_{211} = K_{11}^5, \\
K_{221} &= K_{212} = K_{122} = K_{11}^8, \text{ and} \\
K_{222} &= K_{11}^{12}.
\end{aligned}$$

### 2.5.2 Duplex Reliability Model

The dual memory reliability equation will be of the form:

$$R_{\text{Dual}} = R_M + C_{D1} \times R_M \times (1 - R_M) + C_{D2} \times C_{D3}^2 (1 - R_M)^2$$

where:

$C_{D1}$  = Conditional probability that the first failure will be detected and operation switched to the active standby memory

$C_{D2}$  = Conditional probability that the same address word has not failed

$R_M$  = Reliability of one memory module (i.e., one of the two memory modules in the dual). Same electronics as for the TMR except one additional plane and associated electronics are required for parity checking (i.e., dual memory module has 14 planes).

$C_{D3}$  = Conditional probability that the failure(s) in one memory module are continuously detectable by the memory error detection circuitry, and operation is switched to the other memory module.

Probability  $C_{D1}$  will be greater than  $C_{D3}$ , since  $C_{D1}$  includes only first component part failures. In addition to this, some of the component part failures result in a memory module failure mode which may not be repeatable with respect to the memory error detection. For purposes of this analysis, it will be assumed that  $C_{D1} = C_{D3}$  which will result in a slightly optimistic reliability number for the dual memory.

In the analysis of the dual memory, the memory module electronics were the same as for the TMR with the addition of one memory plane, one inhibit driver, one sense amplifier, and one more bit position in the memory buffer register for purposes of implementing parity checking.

In order for  $C_{D1}$  to be close to unity (i.e., 0.9 or better) it would require more than a single bit parity check (i.e., two or more planes per memory module for parity bits) or some other additional form of memory error detection. For purposes of this analysis and comparison with the TMR, a bare minimum configuration was assumed (i.e., one parity bit).

$C_{D2}$  is found by the following equation, i.e., similar to  $C_{S2}$  in the TMR memory analysis:

$$C_{D2} = \sum_{j=1}^n \sum_{i=1}^n C_j C_i K_{(j,i)},$$

where  $C_i$  is the conditional probability that  $i$  component part failures have occurred in one memory module, given that the memory module has failed.

$K_{(j,i)}$  = Conditional probability that no same word failure has occurred given  $j$  and  $i$  component part failures in two memory modules respectively.

$C_{D2}$  can be evaluated on the basis of no more than two component part failures. This is analogous to what was done in evaluating  $C_{S2}$  and  $C_{S3}$  in the TMR memory analysis.

The value of  $(1-K_{11})$  was determined in a manner similar to  $(1-K_{11})$  for the TMR memory, where:

$$K_{12} = K_{11}^2$$

$$K_{22} = K_{11}^4$$

for both the dual and the TMR memory. (Note: value of  $K_{11}$  for dual memory is not the same as  $K_{11}$  for the TMR memory.)

### 2.5.3 Reliability Estimates

Simulations were performed to derive reliability estimates for the basic duplex memories and for the reconfigured TMR memories. The latter configuration was examined in both TMR and TMR/simplex modes. Relative memory reliability estimates are listed below for the critical mission phase ( $T = 10.8$  hours) in order to compare these configurations.

#### TMR Memory

$\lambda_M$  = Failure rate for one double density memory module plus its associated memory buffer register

$$= 55.2 \times 10^{-6}$$

$$K_{11} = 0.441812$$

$$R_M = 0.9994038$$

$$R_{TMR} = 0.99999941$$

#### Dual Memory

$\lambda_M$  =  $57.6 \times 10^{-6}$  (Same as for TMR with the addition of one plane, one inhibit driver, one sense amplifier, and one more bit position in the MBR.)

$$C_{D2} = 0.275307$$

$C_{D1}$	$R_{Dual}$
1.000000	0.9999994
0.998150*	0.9999977
0.950000	0.9999539
0.900000	0.9999083

\*The value that  $C_{D1}$  must be for  $R_{Dual} = R_{TMR}$ , i.e., 99.8 percent of all first failures must be detected by the memory error detection circuitry.

#### 2.5.4 Conclusions

In order for the dual memory predicted reliability to be equal to the predicted reliability of the TMR memory, it is required that the error detection circuitry in the dual memory have the capability of detecting nearly all first failures that may occur in the memory module, i.e., 99.8 percent of all first failures. The dual memory model utilized for this prediction contains a minimum of error detection circuitry, i.e., one additional memory plane, inhibit driver, sense amplifier, and one additional bit position in the MBR for a one-bit parity check and could not be expected to detect 99.8 percent of all expected first failures in the memory module.

A memory error detection utilizing a one-bit parity check as the only means of error detection could not be expected to detect more than approximately 85 percent of the expected first failures in the memory module. Of this 85 percent, approximately 66 percent comprise a failure mode where detection is repeatable, and approximately 19 percent of the 85 percent involves failures which are by chance detected by parity checking and whose detection by parity checking is not repeatable, i.e., failure would not be detected every time an error occurred. To be able to predict approximately 100 percent detection of the expected first failures in the memory module would require very sophisticated memory error detection circuitry which, in turn, would further degrade the predicted dual memory reliability number.

The reliability prediction for the TMR memory was pessimistic in that it assumes that no compensating failures can occur, i. e., failure is assumed if two or more bits at the same address have failed. This is probably more realistic than assuming 50 percent of these failures are compensating.

The reliability advantage of TMR memories is further strengthened by the feasibility of a TMR/simplex mode of operation and by better operation in a disruptive transient environment. Transient protection techniques for TMR memories are discussed in Section 2.10.

## 2.6 Power Supplies and Distribution

A guidance computer/data adapter designed for a long term, manned mission requires an internal power system with performance characteristics far surpassing those required in forerunning guidance systems. To meet these requirements, the power system must be developed around a proven redundancy concept. Many design approaches have applied redundancy techniques at the component, circuit, or subsystem level. Their relevant merits are discussed in the following paragraphs.

### 2.6.1 Design Approaches

Because of the inflight maintenance requirement, component redundancy may not be applicable except to assure reliability of an individual building block used within a system. Component redundancy, in this case, would affect only the replacement interval for building blocks. On the other hand, a circuit redundancy concept would be a valid approach only if the power distribution system is made highly reliable and various load failures cannot cause secondary failures in the remainder of the system.

Both component and circuit redundancy techniques carry cost, weight, and volume penalties in their usual form. In general, component redundant circuits require four components for each circuit element. In addition, the use of component redundancy for linear circuits is an extremely difficult design problem.

Circuit redundant systems generally employ simple "brute force" duplexing to achieve reliability. In power systems, this means that double the power capability required is available when all circuits are functioning properly. Since simple duplexing, i. e., paralleling of

power circuits, furnishes protection only against undervoltage conditions, additional provisions must be made to insure protection against overvoltage.

A subsystem redundancy design approach results in a power system with several important advantages. For the TMR logic circuits, the power system contains three independent power supply circuits and three independent distribution systems. This can take the form of a triple duplex or a triple simplex configuration. In the triple duplex design, each of the three logic channels receives independent power from two of the three power systems. In the triple-simplex design each logic channel receives independent power from a single source. In the event that one of the power supplies fail, the TMR logic loads will operate in duplex but without the capability of making a true majority decision. This may not be desirable from a reliability standpoint.

For a little extra volume, weight, and cost penalty, a triple-duplex design can be realized. This configuration, shown in Figure 33, results in double-sized, power supplies, but the computer adapter logic configuration remains TMR, even with a power supply failure.

A disadvantage of either the triple-simplex or triple-duplex supply configuration is that protection is required against overvoltage. A power supply failure must not result in stress failures within the logic channel loads. For this reason, the control portions of each power supply are made duplex redundant. The converter portions make use of circuit techniques developed for the Saturn-V Launch Vehicle Data Adapter power supplies. These are designed not to fail in an overvoltage mode.

To prevent power supply load-sharing problems, it is necessary for each feedback control loop to sample both the isolation diode input voltage and the respective bus voltage. With this arrangement, a short circuit in an individual distribution system will not cause excessive voltage rises on the other distribution lines. Further precaution against load sharing problems can be taken by providing energy coupling between primary power sources. This can be accomplished by using a multiple-winding, common core filter inductor to couple transient energy between independent power lines, thereby stabilizing the process of transferring loads between power supplies.

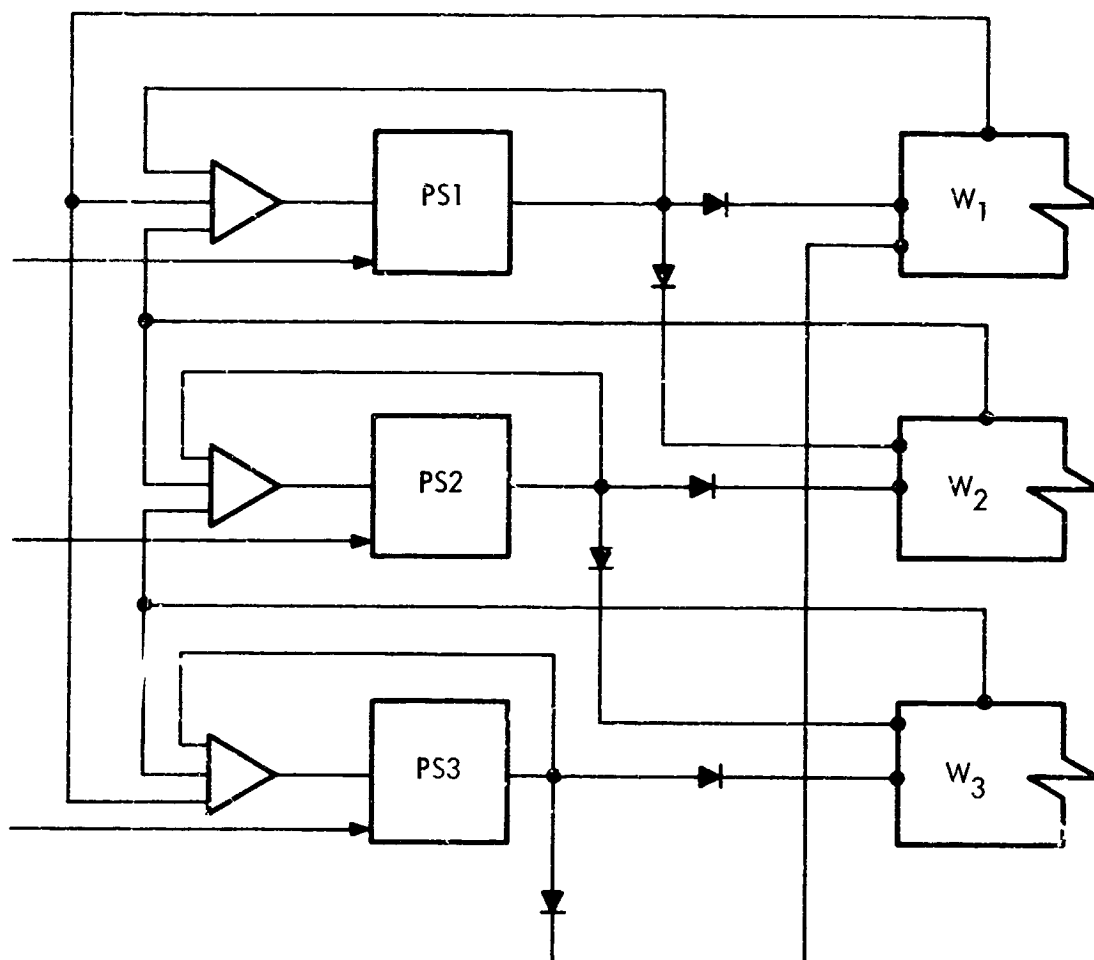


Figure 33. Triplex-Duplex Power System

### 2.6.2 Power Supply Switching

There are three reasons for providing some form of a power switching arrangement between the primary sources and the loads:

- 1) To provide proper turn-on and turn-off sequencing for loads such as destructive readout memories.
- 2) To permit removal of a power supply because of a failure in the supply.
- 3) To permit removal of a section of the load because of a power failure in the load itself.

The switching combinations that are possible between power supplies and loads require the use of remote error sensing circuits. These should be designed to insure proper voltage regulation at the various distribution loads.

To switch the power supply outputs, the isolation diodes shown in Figure 33 can be replaced by power transistors. The base drive circuitry for these power switches requires some auxiliary voltage sources to insure sufficient forward bias for "on" switches and to prevent base-emitter breakdown of "off" switches. The remote sensing lines must also be switched or otherwise disabled. One of the several techniques used for low-level analog switching may prove to be suitable.

### 2.6.3 Recommendations

In summary, the power system described includes three simplex power supplies, duplexed into three independent power distribution systems using power switching transistors. Each simplex supply includes duplex error amplifiers to prevent overvoltage failures. All remote sense lines are capable of being switched to permit removal of any power supply or any load. A single power supply failure results in two simplex powered loads and one duplex powered load. A single short circuit load failure results in one operational power supply feeding two loads.

### 2.6.4 Power Requirements

Based on the preceding requirements for a triple-duplexed power system, the power requirements for each of the three TMR portions of the computer-adaptor equipment are summarized in Table 8.

TABLE 8 — Regulated DC Power Per Section

Voltage (dc)	Load Current (amperes)	Load Power (watts)
+ 20	0.84	16.8
+ 12	0.092	1.1
+ 6	3.44	20.6
- 3	0.10	0.3

### 2.6.5 Power Supply Circuit Configurations

Since each power supply output is required to drive two loads, the design centers for each voltage will be twice that given in Table 8. This table also shows that two of the loads are very light in comparison to the others. Because of this, the use of independent power supplies for these outputs is not recommended. This decision is based on both the design cost and hardware standpoint. The best balance between component cost, manufacturability, testing, and maintenance is obtained by using an interrelated system. This is shown in Figure 34. These blocks represent one-third of the total power supply system.

The series regulator in Figure 34 must be designed to prevent an overvoltage at the output. This is accomplished most economically by providing duplexed error signal amplifiers and a dual series pass element.

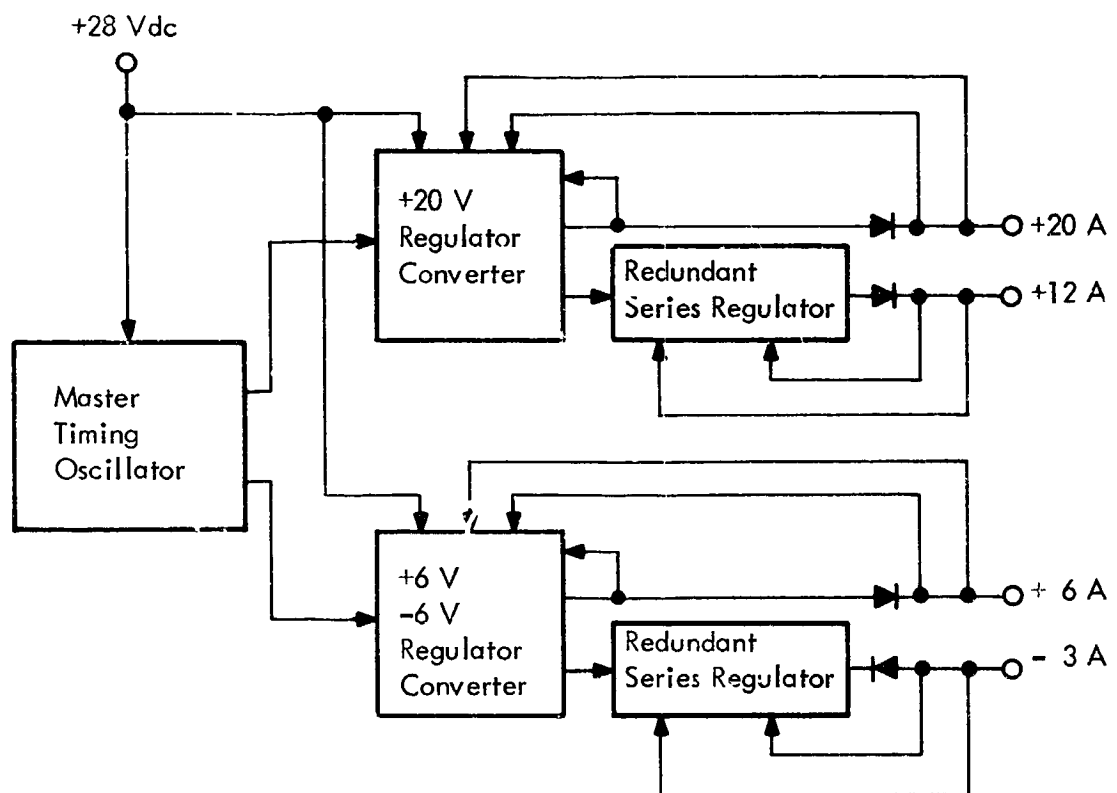


Figure 34. Interrelated Power System

The entire power supply system will require three master oscillators, six regulated DC-to-DC converters with duplexed amplifiers, six redundant series regulators, twelve isolation and/or power switching elements, and twenty-four remote sense line switches. Since the power levels are similar for the two types of converter-regulator chains, multiple use can be made of many existing building blocks used in the computer-adaptor equipment. Component part requirements are given in Table 9.

**TABLE 9 — Power System Component Count**

Components	Quantity
Small Signal Semiconductors and Resistors	1194
Power Semiconductors	42
Magnetic Components	24
Capacitors - Ceramic and Tantalum	118
Reference Network Components	42
Total Count	1420

The volume and weight estimates of each power supply section are based on the use of discrete components, with an operating frequency of 100 kc/s for the converter portions. A reduction of approximately 20 percent in volume can be realized in integrated circuit amplifiers, modulators, and control circuits are utilized. Power supply size estimates are based on the use of three identical packages. Each one contains two basic converters which supply four outputs and the sequencing controls necessary for those outputs. Each unit will be contained in a volume of approximately 55 cubic inches and will weigh 3 pounds.

## 2.7 Grounding

### 2.7.1 Saturn-V Grounding

The general grounding system of the Saturn-V computer and data adapter, consisting of a regulated d-c return and a filtered power return, was retained in the AES computer subsystem. As shown in Figure 35, the common vehicle ground for the AES system is brought into the computer subsystem in duplex form through an RFI filter. The outputs of the RFI filter are "commoned" in a ground plane designated as the filtered power return, are capacitively coupled to the subsystem chassis, and are routed through a transient decoupler to the triplex power supplies. The secondaries of the power supply transformers are "commoned" in a second ground plane designated as the regulated d-c return, which in turn is routed in duplex form from the computer subsystem to the common vehicle ground.

The filtered power return is used as a reference for the 28-volt d-c output driver circuits and for elapsed time indicators. Discrete outputs, discrete inputs, and d-c interrupts are referenced to the filtered power return. The ground plane is located physically in the back-panel multilayer interconnection board.

The regulated d-c return is used as a reference for signal and power supply ground. Any signals to other equipment in the command module which are referenced to the regulated d-c return will be transformer coupled or floated within that equipment. The regulated d-c return consists of ground planes in the back-panel multilayer board and in each of the logic module multilayer boards.

### 2.7.2 AES Grounding Modifications

Certain modifications to the Saturn-V grounding details were made. In Figure 36, the module reference for the memory is shown as three separate ground planes commoned at a single point in the back-panel ground plane. The connection to the common vehicle ground is also made at this same point on the back-panel ground plane. This representation of the memory grounding is meant to indicate that special consideration was given the physical location and electrical connection of the memory ground reference to minimize the noise effects of equipment ground current distributions on the AES memory. Isolation of the three channel ground planes of the memory in this

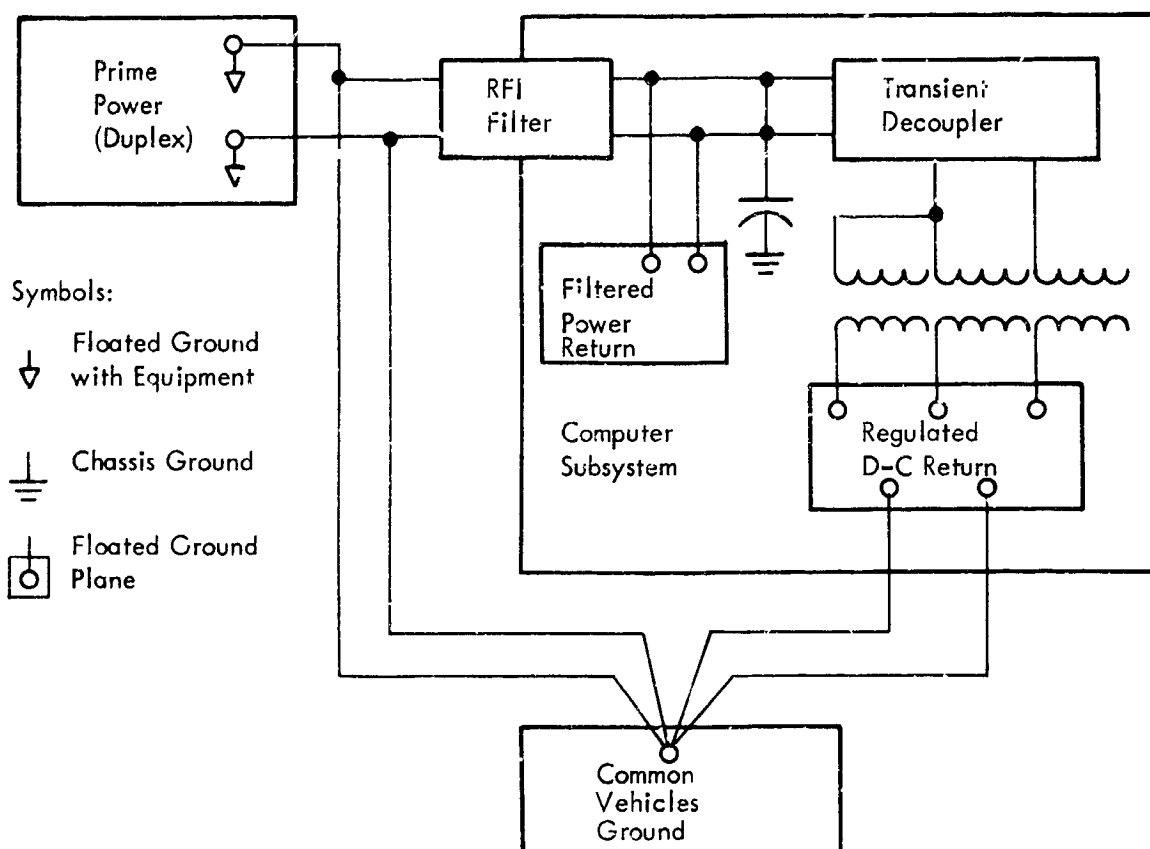


Figure 35. Grounding System

manner also minimizes the probability that a voltage transient of external origin will affect all three memory channels, since cross-channel coupling of transient currents is minimized.

The ground planes of the remaining modules in the computer-data adapter subsystem are shown as single planes although each module exists physically as three individual simplex subassemblies containing individual ground planes in their respective multilayer

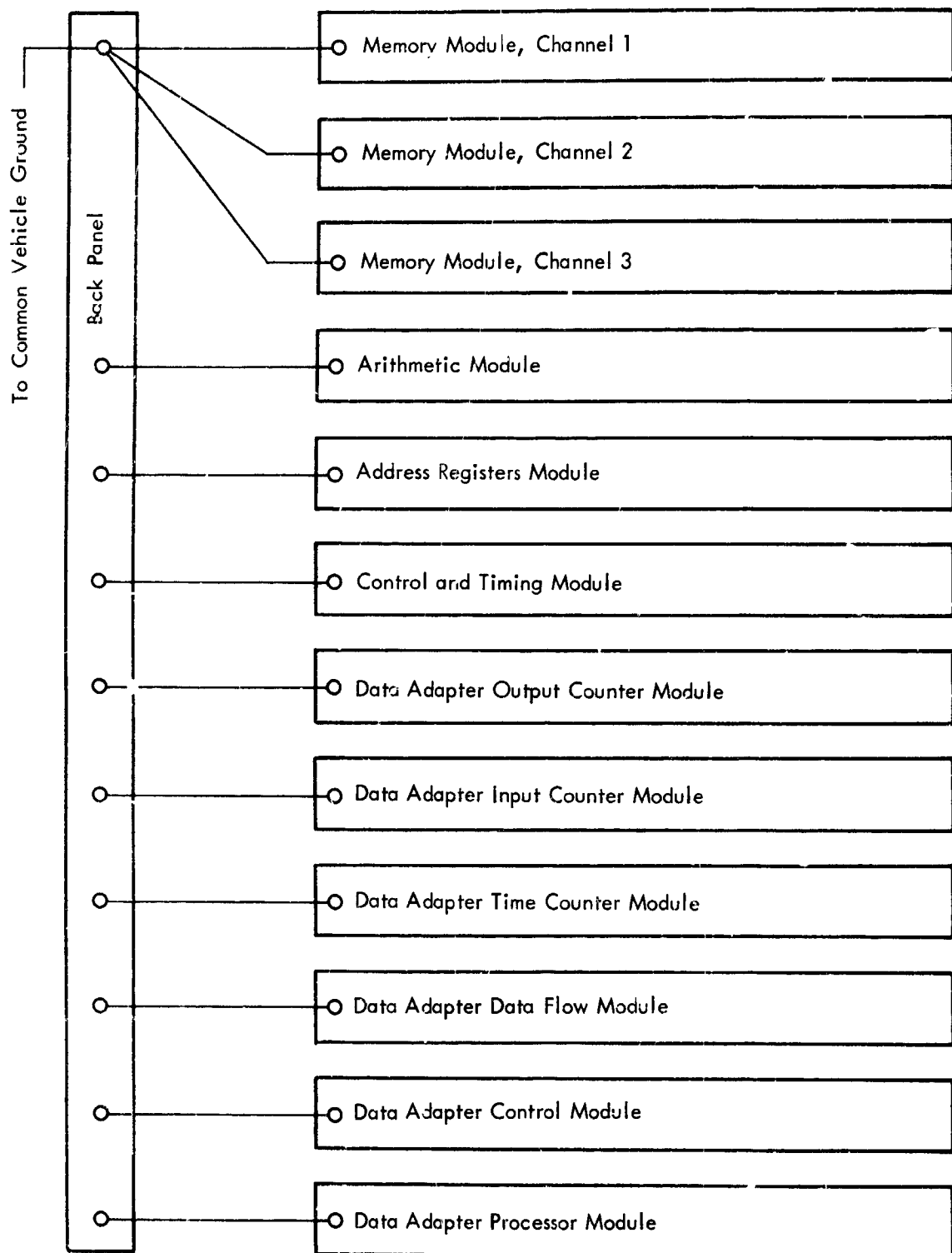


Figure 36. Regulated DC Return Ground Planes

interconnection boards. This representation of the module grounding is meant to indicate that there was no attempt made to isolate the individual ground planes as in the memory area.

An additional ground plane is provided in each simplex module, as shown in Figure 37 to isolate the logic ground currents from the voted intermodule signal returns. The ideal intermodule interconnection technique for ground current isolation would be twisted signal-to-ground pairs except that the number of module interconnections becomes prohibitive. The technique shown in Figure 37 effectively contains the logic ground currents in the module and separated from the voted interconnection currents. The regulated d-c return ground plane in the back-panel interconnection board contains mainly interconnection signal return currents and power currents.

### 2.7.3 Interface Circuits

There are four basic types of circuits which interface the computer subsystem to the other AES subsystems:

- 1) Type D - Discrete inputs,
- 2) Type C - Discrete outputs,
- 3) Type Y - Transformer coupled inputs
- 4) Type X - Transformer coupled outputs.

The interface characteristics for these interface circuits are the same as those of the Apollo backup data adapter except that the AES circuits will be component-redundant. Simplex versions of these circuits and some of their more important characteristics, including the manner in which they are tied into the AES grounding system, are described in the following paragraphs.

A simplex example of a typical AES discrete input circuit is shown in Figure 38. Note that the ground reference from the driving AES subsystem for the 28-volt d-c discrete is not routed along with the signal. This separate routing of signal and reference simplified Apollo interface wiring, and the resulting sensitivity to noise pickup was not

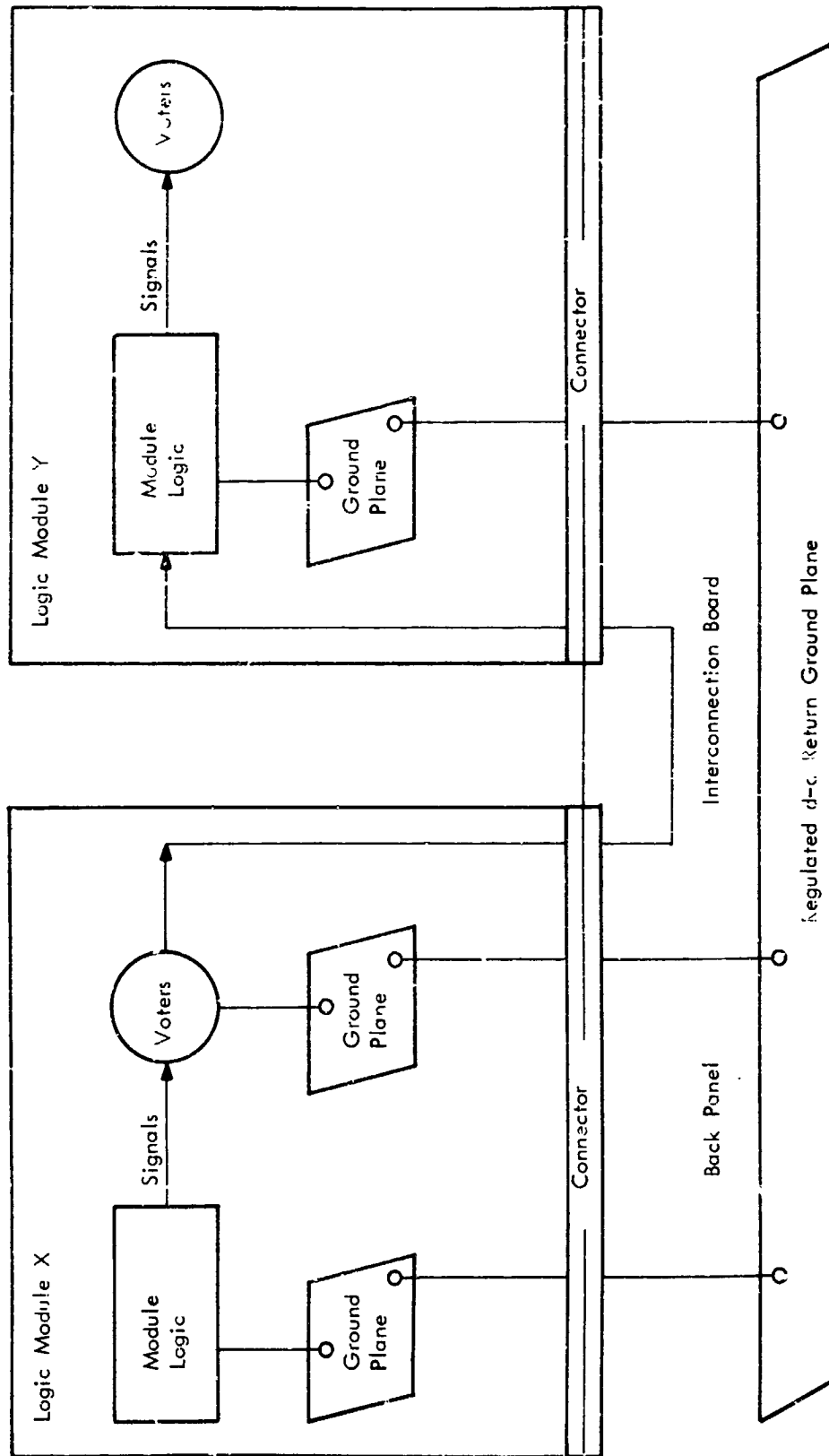


Figure 37. Module Ground Planes

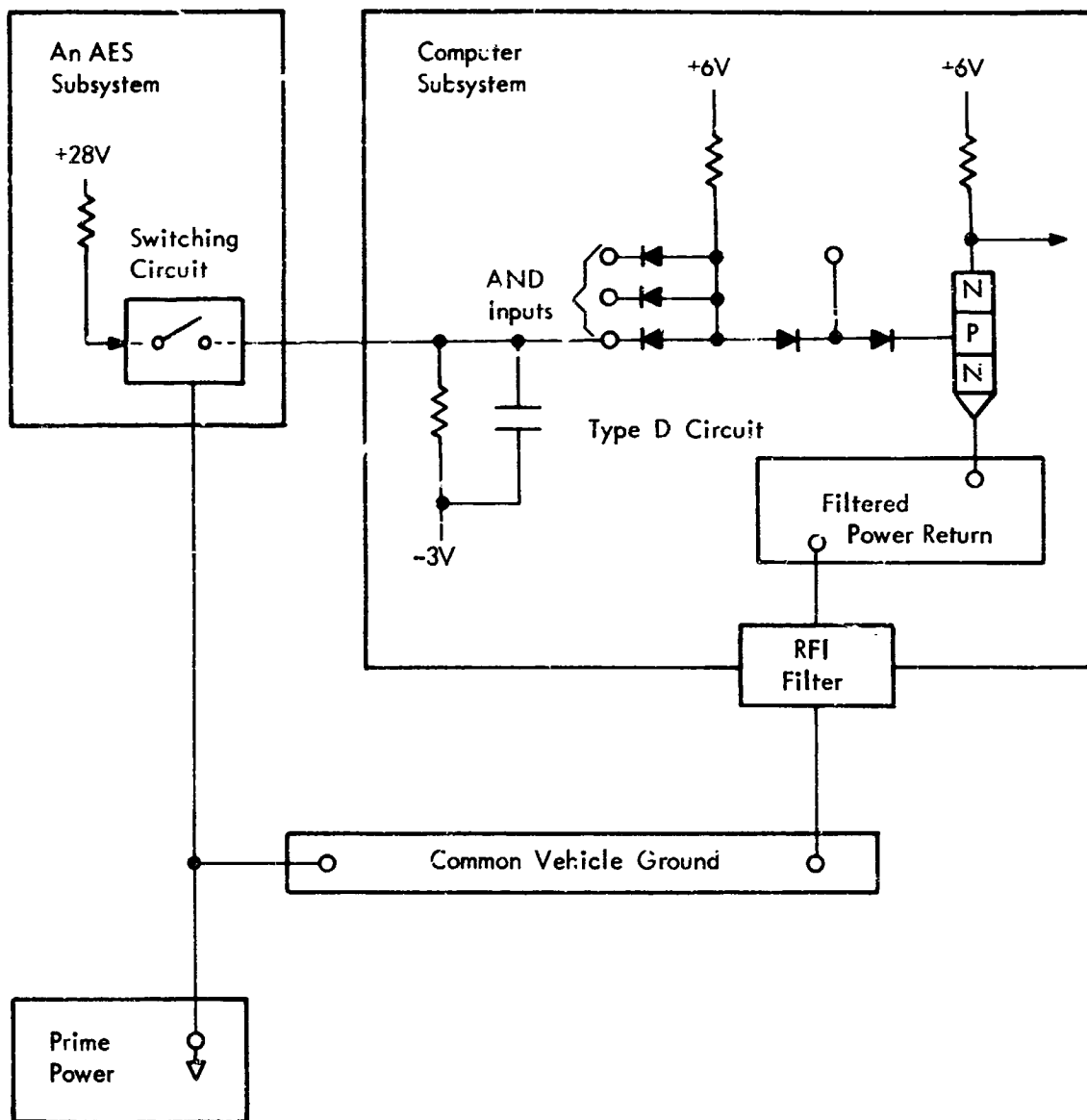


Figure 38. Discrete Input Circuit

considered to be critical in the case of d-c signals. The circuit characteristics of the discrete input signals are:

- |    |                    |   |        |                       |
|----|--------------------|---|--------|-----------------------|
| 1) | Input signal level | - | "one"  | 28 $\pm$ 11 volts d-c |
|    |                    |   | "zero" | 0 $\pm$ 2 volts d-c   |
| 2) | Source impedance   | - | "one"  | 4,000 ohms            |
|    |                    |   | "zero" | open                  |
| 3) | Load impedance     | - | "one"  | 22,000 ohms           |
|    |                    |   | "zero" | 22,000 ohms           |

A simplex example of a typical AES discrete output circuit is shown in Figure 39. Again it was not considered necessary to route the ground reference along with the d-c signal. The circuit characteristics of the discrete output signals are:

- |    |                   |   |        |                                |
|----|-------------------|---|--------|--------------------------------|
| 1) | Source impedance  | - | "one"  | 3,000 ohms maximum             |
|    |                   |   | "zero" | 500,000 ohms maximum           |
| 2) | Collector current | - | "one"  | 5 milliamperes maximum         |
| 3) | Output            | - | "zero" | 0 milliamperes at 40 volts d-c |

A simplex example of a typical AES transformer coupled pulse input circuit is shown in Figure 40. The regulated d-c return is used as the ground reference for these circuits, since the transformer provides ground decoupling between the computer subsystem and the driving subsystem. The circuit characteristics of the pulse input signals are:

- |    |                    |   |        |                        |
|----|--------------------|---|--------|------------------------|
| 1) | Input signal level | - | "one"  | 7 $\pm$ 3 volts        |
| 2) | Signal pulse width | - |        | 4 $\pm$ 2 microseconds |
| 3) | Source impedance   | - | "one"  | 100 ohms               |
|    |                    |   | "zero" | 10 ohms                |
| 4) | Load impedance     | - | "one"  | 200 ohms               |
|    |                    |   | "zero" | 20 ohms.               |

A simplex example of a typical AES transformer coupled pulse output circuit is shown in Figure 41. Again the regulated d-c return is

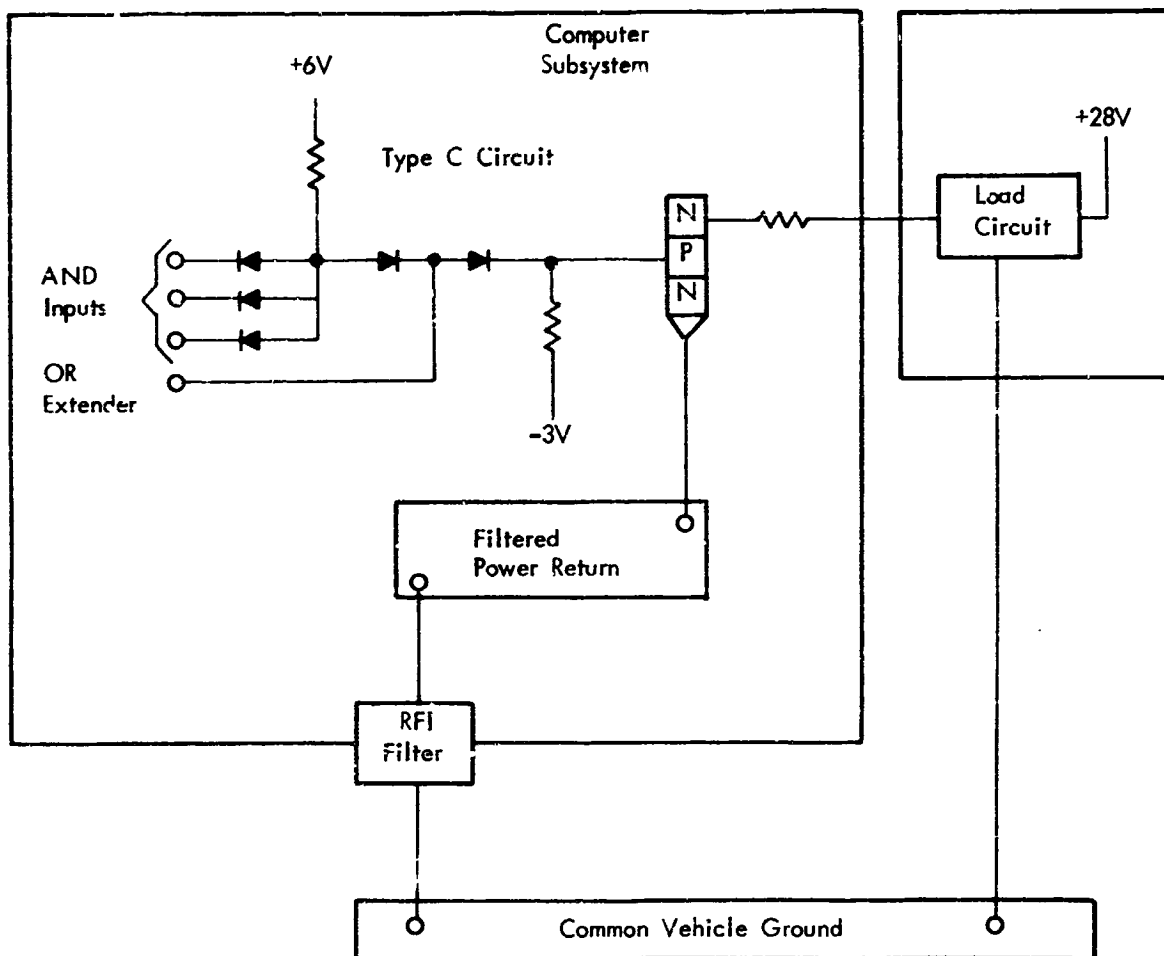


Figure 39. Discrete Output Circuit

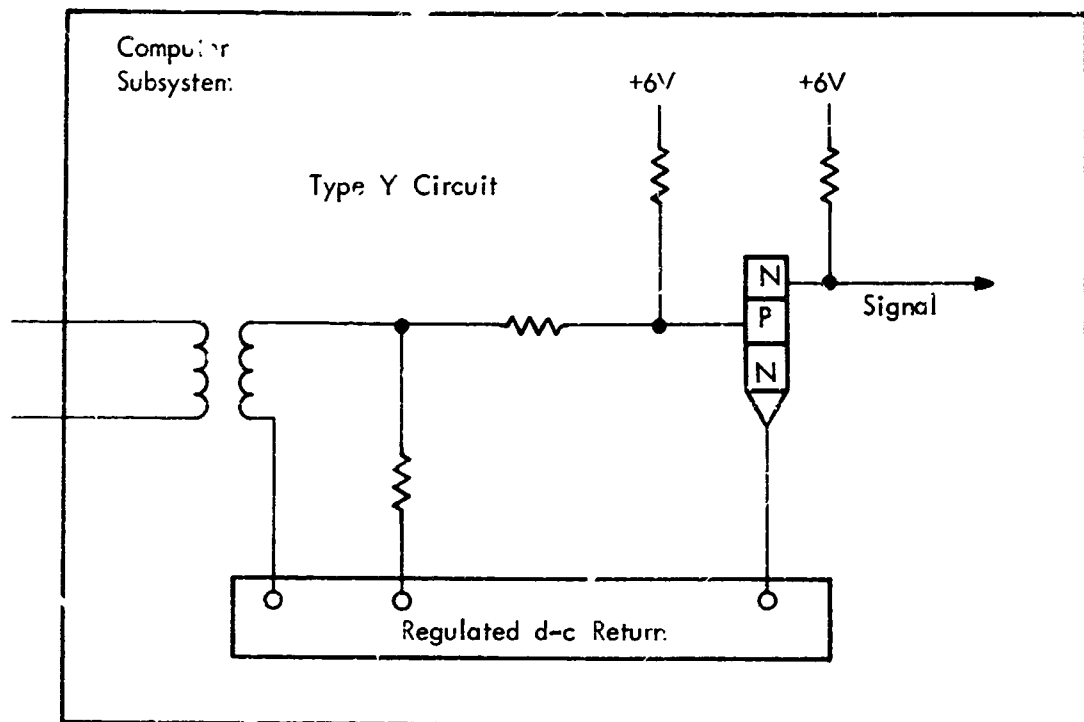


Figure 40. Pulse Input Circuit

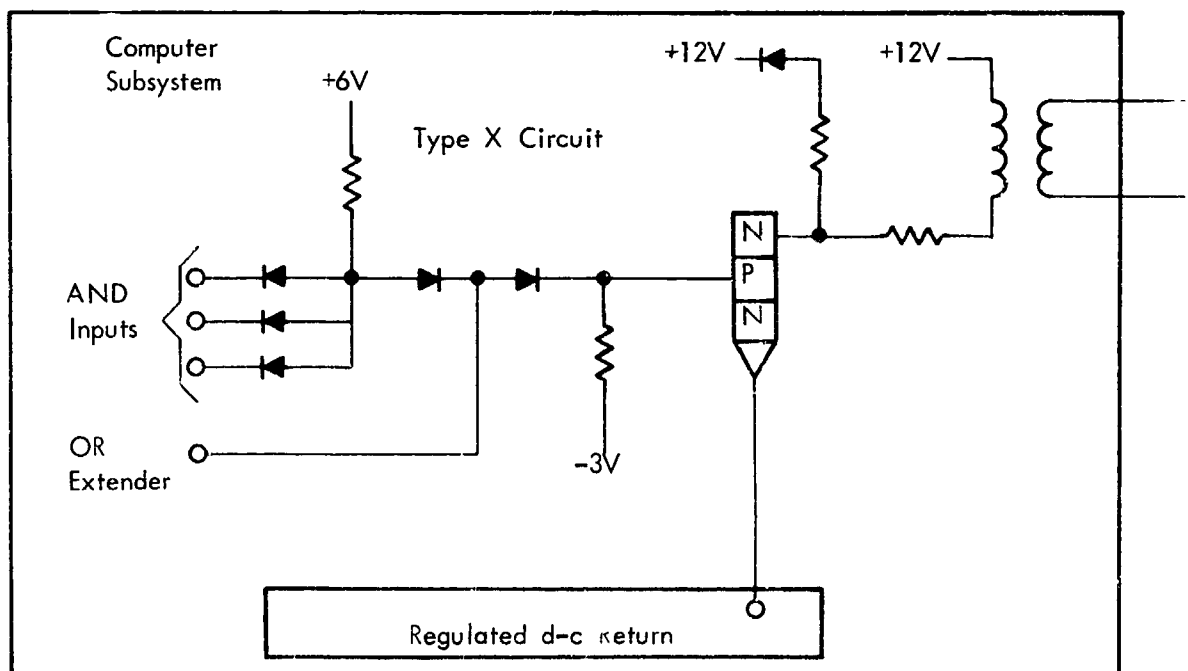


Figure 41. Pulse Output Circuit

used as the ground reference. The circuit characteristics of the pulse output signals are:

- |    |                       |        |                          |
|----|-----------------------|--------|--------------------------|
| 1) | Output signal level - | "one"  | $7 \pm 3$ volts          |
| 2) | Signal pulse width -  |        | 0.25 to 6.0 microseconds |
| 3) | Source impedance -    | "one"  | 100 ohms                 |
|    |                       | "zero" | 10 ohms                  |
| 4) | Load impedance -      | "one"  | 100 to 500 ohms          |
|    |                       | "zero" | 20 ohms.                 |

## 2.8 TMR/Simplex Mode

A new operating mode for the AES system was considered during the study in which one or more modules in the computer and data adapter operate simplex while the remaining modules operate TMR. This mode would be useful not only for equipment checkout as channel and module switching modes are used in the Saturn-V program but would provide an increase in reliability over the basic TMR mode as described in the following sections.

### 2.8.1 Reliability Considerations

The expression for the basic reliability of a TMR module without regard to logical direction of failure is

$$R_{TM} = 3 R_c^2 - 2 R_c^3,$$

where  $R_c$  is the reliability of one channel of the module. Assuming a constant failure rate ( $\lambda$ ) for the module,

$$R_c = e^{-\lambda t} = e^{-t/MTBF},$$

where MTBF is the mean time between failures of each channel of the TMR module.

The reliability curves for the simplex module and for the TMR module are plotted in Figure 42 against normalized time ( $t/MTBF$ ). Since the curves cross at  $t = 0.69 MTBF$ , it is obvious that TMR

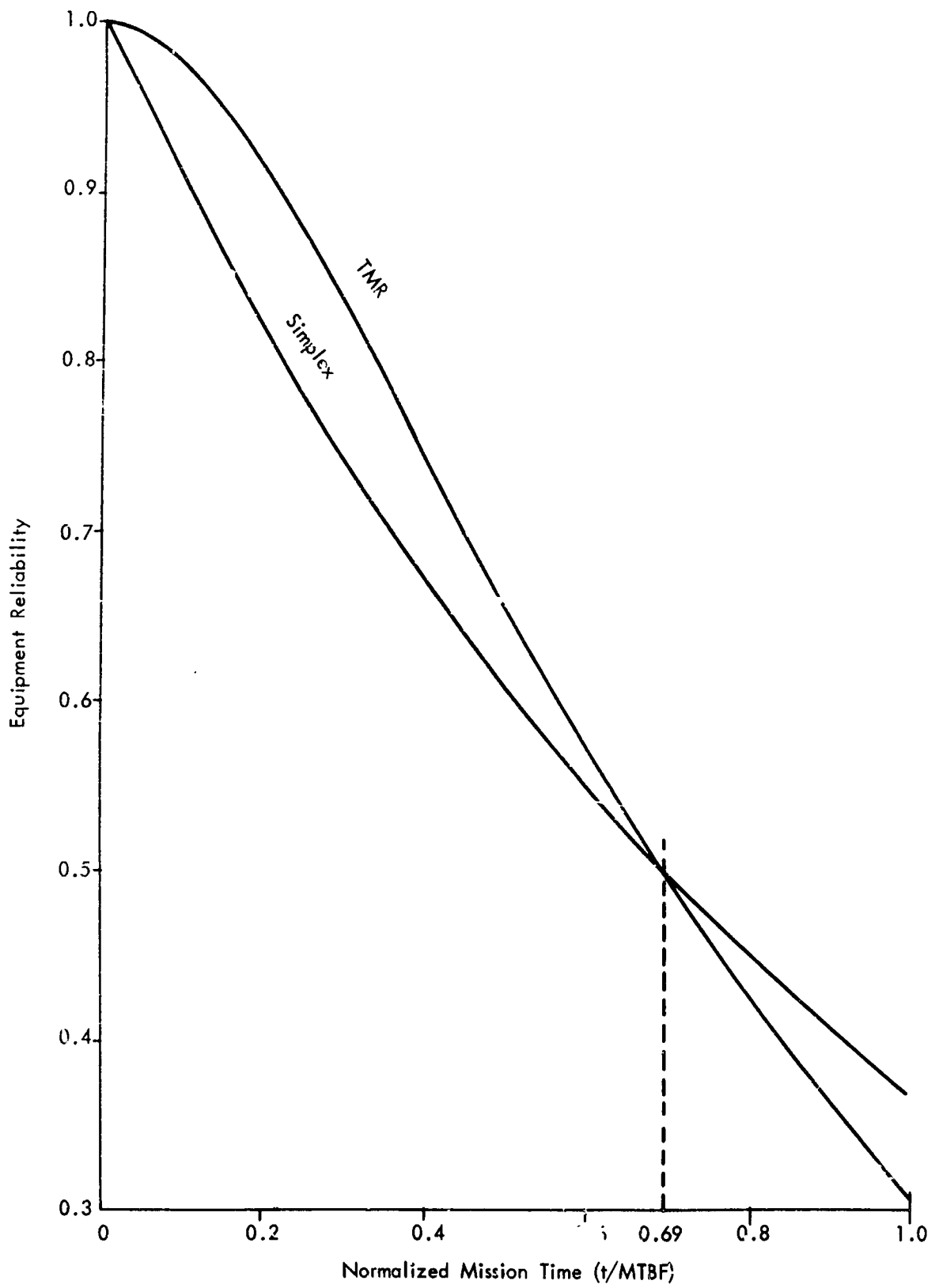


Figure 42. Generalized Reliability Curves

configurations should be used only in applications where mission time is short compared to the MTBF of the simplex channel unless maintenance is permitted during the mission.

Note that if a failure occurs in one channel, both the remaining channels must continue to operate correctly. Once a failure has occurred in a module, therefore, the reliability of that module is less than that of a simplex channel. For example, if a failure occurs in channel 1, the reliability of the module becomes  $R_2 R_3 = R_c^2$  while the reliability of a channel is  $R_c$ . A reliability improvement should be possible by switching out one of the remaining unfailed channels after a failure has occurred in a module and thereby operating that module simplex while the remainder of the computer and data adapter operate TMR. The choice of which of the good channels to switch out is arbitrary

### 2.8.2 Basic TMR/Simplex Reliability

The reliability of a TMR module in the TMR/simplex mode can be derived by adding the probabilities of operating states as was done for the basic TMR mode in Section 2.1.2. A somewhat more rigorous method was used, however, as follows.

Denote the phase or mission time period for which the reliability is to be calculated by the constant  $T$  and operating time within this period by the variable  $t$ . Assume that a first malfunction occurs at some time  $\tau$  during the phase or mission, where  $0 \leq \tau \leq T$ .

The probability that one or more malfunctions will occur by time  $t$ , assuming constant failure rate  $\lambda$ , can be represented by the unreliability expression

$$U = (1 - e^{-3\lambda t}).$$

The probability density of a failure occurring at the specified time  $\tau$  is

$$u = \left. \frac{dU}{dt} \right|_{t=\tau} = 3\lambda e^{-3\lambda\tau}.$$

The probability that a failure will occur during any increment of time,  $d\tau$ , at a specified time  $\tau$  is

$$u d\tau = 3\lambda e^{-3\lambda\tau} d\tau$$

Now assume that, when the first failure occurs, the faulty channel of the module plus one of the good channels are switched off. The probability that the module is operating at the end of the time period  $T$  is then given by the product of the probability that a failure occurs at time  $\tau$  ( $\lambda d\tau$ ) and the conditional probability that if a failure does occur at time  $\tau$  and the switching action is accomplished, then the remaining good module operates for the remainder of the phase or mission time ( $e^{-\lambda(T-\tau)}$ ).

$$3\lambda e^{-3\lambda\tau} d\tau (e^{-\lambda(T-\tau)})$$

$$3\lambda e^{-2\lambda\tau} \cdot e^{-\lambda t} d\tau.$$

Since the time of first failure could occur at any specific time during the phase or mission, the reliability expression derived above must be summed for all specific times during the period  $T$ , or

$$3\lambda e^{-\lambda t T} \int_0^T e^{-2\lambda\tau} d\tau.$$

Solving the integral expression and substituting  $R_c$  (reliability of one channel of the TMR module) for the exponential  $e^{-\lambda T}$ ,

$$3/2 R_c - 3/2 R_c^3.$$

This is the expression for the probability that the module is operating at the end of the phase or mission, assuming that a failure occurs during the period of the phase or mission. The reliability of the TMR module in the TMR/simplex mode is derived by adding to this expression the probability that no failures occur during the time period, or

$$\begin{aligned} RTSM &= 3/2 R_c - 3/2 R_c^3 + R_c^3 \\ &= 3/2 R_c - 1/2 R_c^3. \end{aligned}$$

This expression is identical to the expression for TMR reliability without the TMR/simplex mode but assumes with equal probabilities that two failures may occur in the same or opposite directions ( $P(o) = 1/2$ ). The TMR/simplex mode therefore effectively forces compensating errors in different channels of the TMR module 50 percent of the time.

### 2.8.3 Ultimate TMR/Simplex Reliability

In the derivation of the reliability expression for the TMR/simplex mode it was assumed that, when a failure occurred, a good channel of the module was switched off along with the defective channel. If it is possible to use this channel as a spare in case the operating channel of the switched TMR module in turn fails, then the ultimate reliability provided by a TMR/simplex mode can be achieved.

Assuming, conservatively, that the off-time failure rate of the "spare" channel is equal to the operating failure rate of a channel, then the reliability of a TMR channel in the TMR/simplex mode (and using the "spare" channel) is

$$R_{TM} = 1 - (1 - R_c)^3.$$

This equation expresses the fact that all three channels must fail to fail the TMR module. It is identical to the expression for TMR reliability without the TMR/simplex mode but assumes that compensating errors always occur in related portions of the three channels.

The reliability of the basic TMR/simplex mode and the "ultimate" reliability of this mode are compared in Figure 43 with the reliability of the basic TMR mode. Reliability is shown plotted against normalized time on a time scale representing a few hundred operating hours.

## 2.9 Reorganized Subsystem

The reorganized computer subsystem was derived from the basic subsystem consisting of the Saturn-V computer and a redundant version of the Apollo backup data adapter by reconfiguring certain performance constraining areas (such as the oscillator, memory, and power supplies) and by repartitioning the basic computer and data adapter into replaceable modules suitable for error diagnosis and replacement. This reorganized subsystem was then examined to determine to what extent it met the functional and availability requirements of the 90-day AES-EPO mission.

### 2.9.1 Computer Description

The attempts at partitioning the computer into modules resulted in a four-module computer with the memory contained as one of the

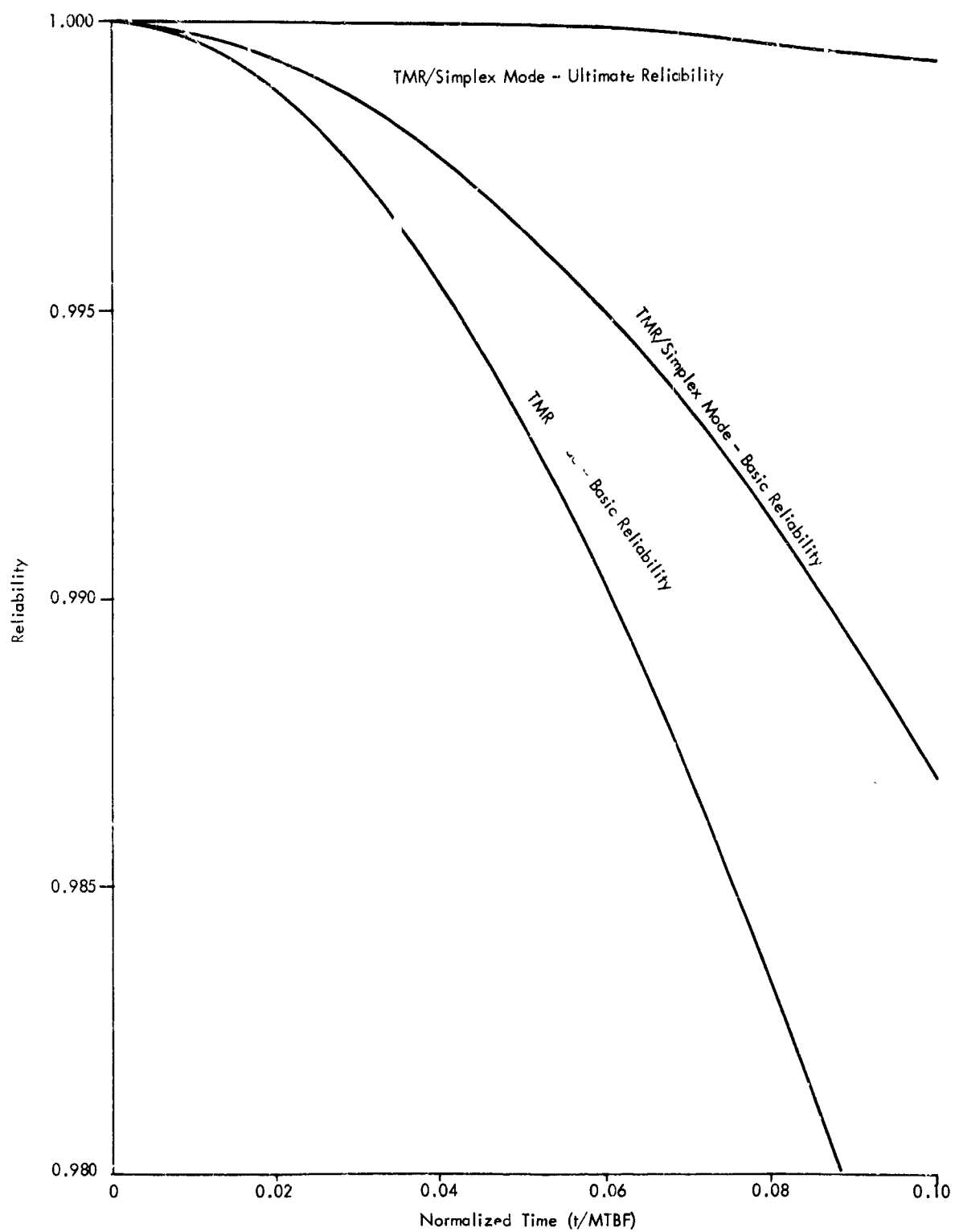


Figure 43. Reliability Comparison (TMR and TMR/Simplex)

modules. These four modules (memory and memory interface, arithmetic, address registers, and control and timing) required a total of 120 voters to be assigned to the intermodule interface signals. Using the Saturn logic as a reference, the logic was "sized" using a typical DTL integrated circuit family. Since no voter or disagreement detector circuits are presently available in this circuit family, it was assumed that each could be contained on an integrated circuit chip or flat pack. The subsequent module sizing data are tabulated in Table 10. Figure 44 indicates how the Saturn computer could be partitioned into the modules as described.

TABLE 10 - Computer Sizing

Module No.	No. of Chips			No. of Inputs-Outputs			
	Logic	Voter	Total	Inputs	Outputs	Voter Interconnection	Total
1	72*	34	106*	78	17	51	146
2	169**	18	187**	72	9	27	108
3	59	80	139	59	40	120	219
4	83	92	175	36	46	138	220

\* Does not include memory electronics

\*\* Does not include delay line (or shift register chips)

The partitioning of the computer logic into modules was functional in nature. For example, module number 2 contains all the arithmetic logic. This allows the maximum intra-connection of the logic within a given module and, therefore, reduces the interconnection between modules. Module 2 is a classic example because it contains the most logic of any module and the least interconnections. Only nine signals are outputs and require voters.

In theory, the more signals that are voted, the more reliable the machine. However, the voters also have a failure rate and a situation where more voter failures occur than logic failures cannot be tolerated. Also, it has been demonstrated that the TMR reliability is maximized when the modules are the same size, i.e., their simplex reliabilities are equal.

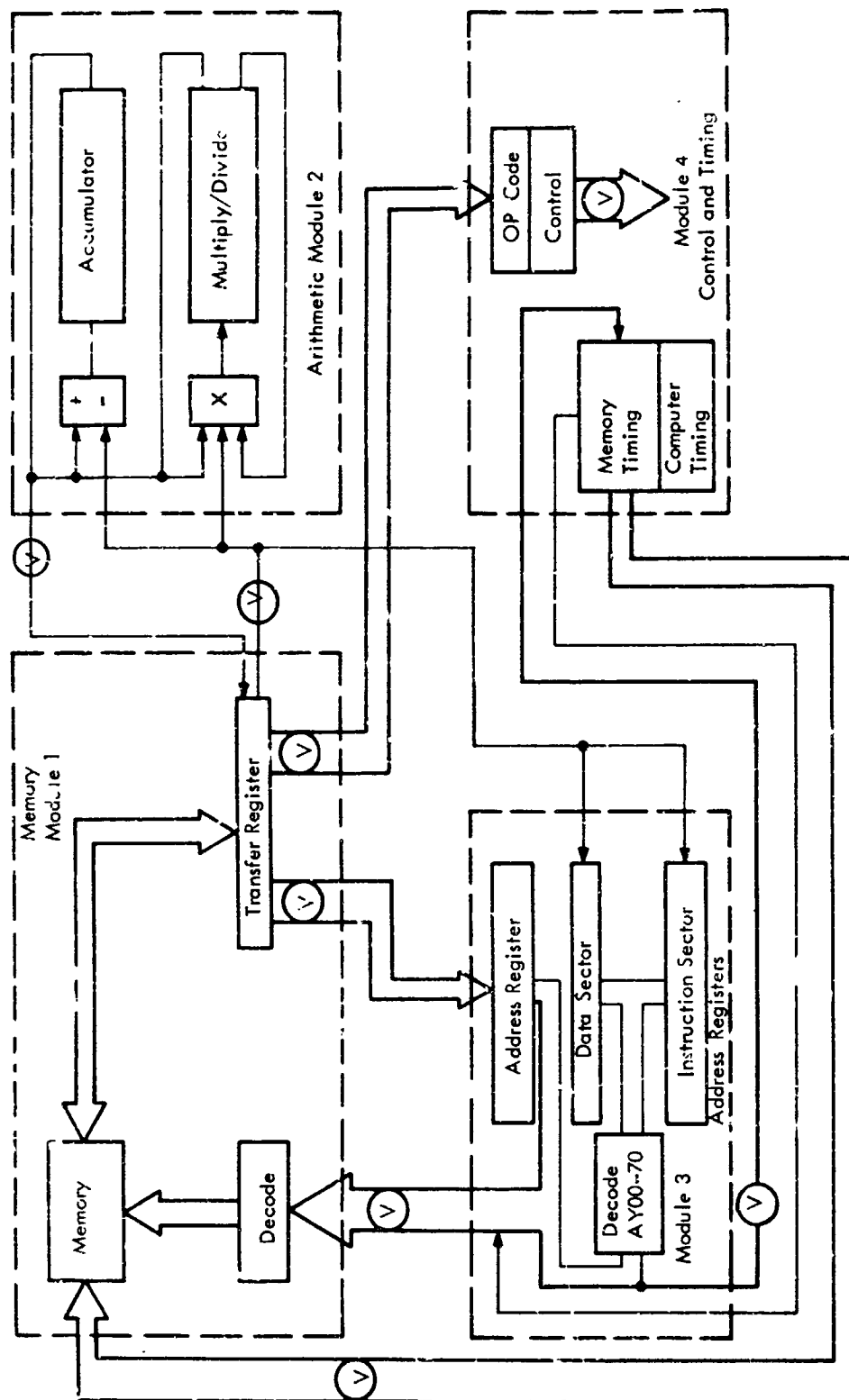


Figure 44. Four-Module Partitioning of the Saturn-V Computer

In practice, the partitioning and voter assignment are a series of trade-offs. Unfortunately, no tool is presently available which will do this and maximize the system reliability at the same time. This can be done only through a trial and error procedure where the reliability of a given partitioning is computed. Obviously, it is impossible to do this for all possible partitionings. The final result was the selection of the partitioning with the least number of voters which yields the desired reliability.

In an attempt to simplify the data adapter portion of the Apollo computer, a study was made of one possible means of increasing the central processor speed. In this study, the central processor organization was restricted to be identical to that employed in the Saturn-V computer. An increase of four times in the speed was found to be feasible using state-of-the-art components. The three major areas affected would be the memory, the logic circuits, and the glass delay line storage elements. The requirements in these areas for a "times four" computer are:

- 1) Memory - The memory proposed for the AES is a double density Saturn-V array which uses conventional toroidal cores. Unlike the Saturn-V system, the memories will not possess the duplex capability. This scheme will be replaced with a TMR organization that will also allow simplex operation of the three redundant computers. Each memory will contain 8192 28-bit words and will be augmented with an on-board memory load capability. Memory cycle time will be 2.5 nanoseconds.

Parity checking is not required when operating in the TMR mode, since each bit of the 14-bit parallel word is voted. The parity check capability is included, however, to provide error indications when operating as independent simplex systems. In the simplex mode of operation, the three memory modules operate independently with their respective computers. Thus, each computing system has its own 8192 word memory.

When in the TMR mode of operation, each output of the 14-bit positions of the buffer register is voted. Accordingly, the contents of each memory are restored correctly had a disagreement occurred in any one.

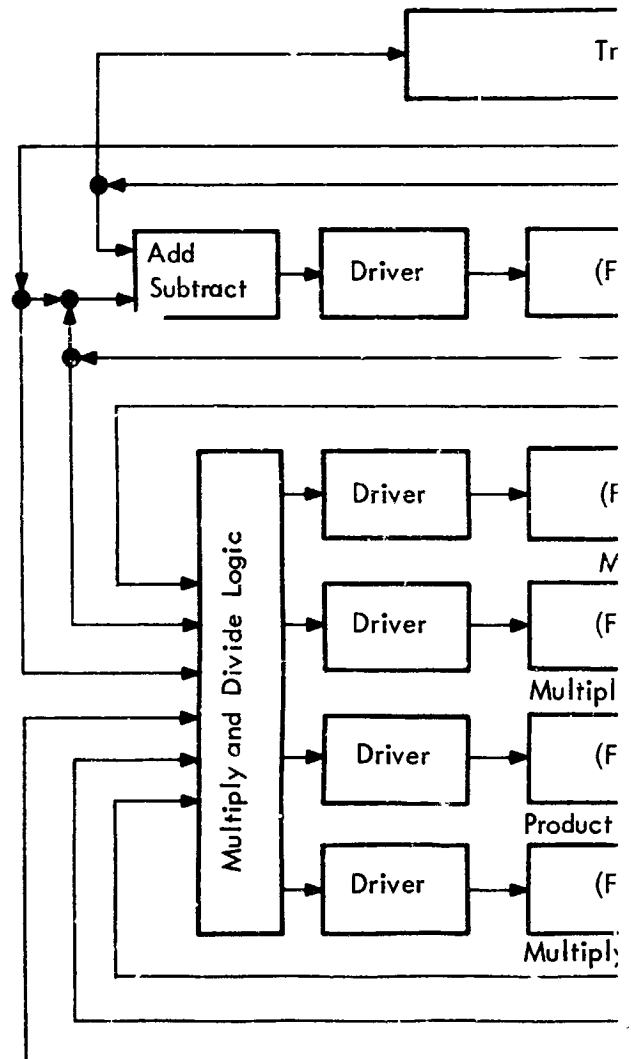
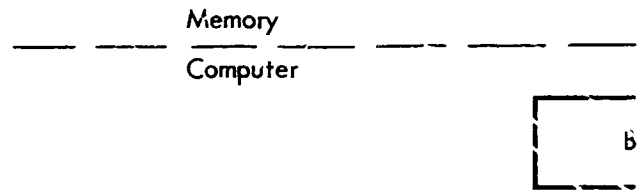
- 2) Logic Circuits - The logic circuits have approximately 50 nanoseconds delay per stage. Integrated circuits are available from many sources which would satisfy this requirement.

- 3) Delay Lines - The delay lines have a 2 megacycle bit rate. This requirement may be satisfied in a number of ways. The present Saturn-V computer uses two glass delay lines with four channels of information per line. For an equivalent 2-megacycle bit rate, eight of these lines would be required in the "times four" computer. An integrated circuit shift register using field effect transistors (FET) is available with a reliable operating range from 50 kilocycles to 2 megacycles. These shift registers duplicate the function of the glass delay lines and have the advantage of being much smaller and less critical to variations in clocking frequency. Each computer will use eight of these devices to provide the required arithmetic registers.

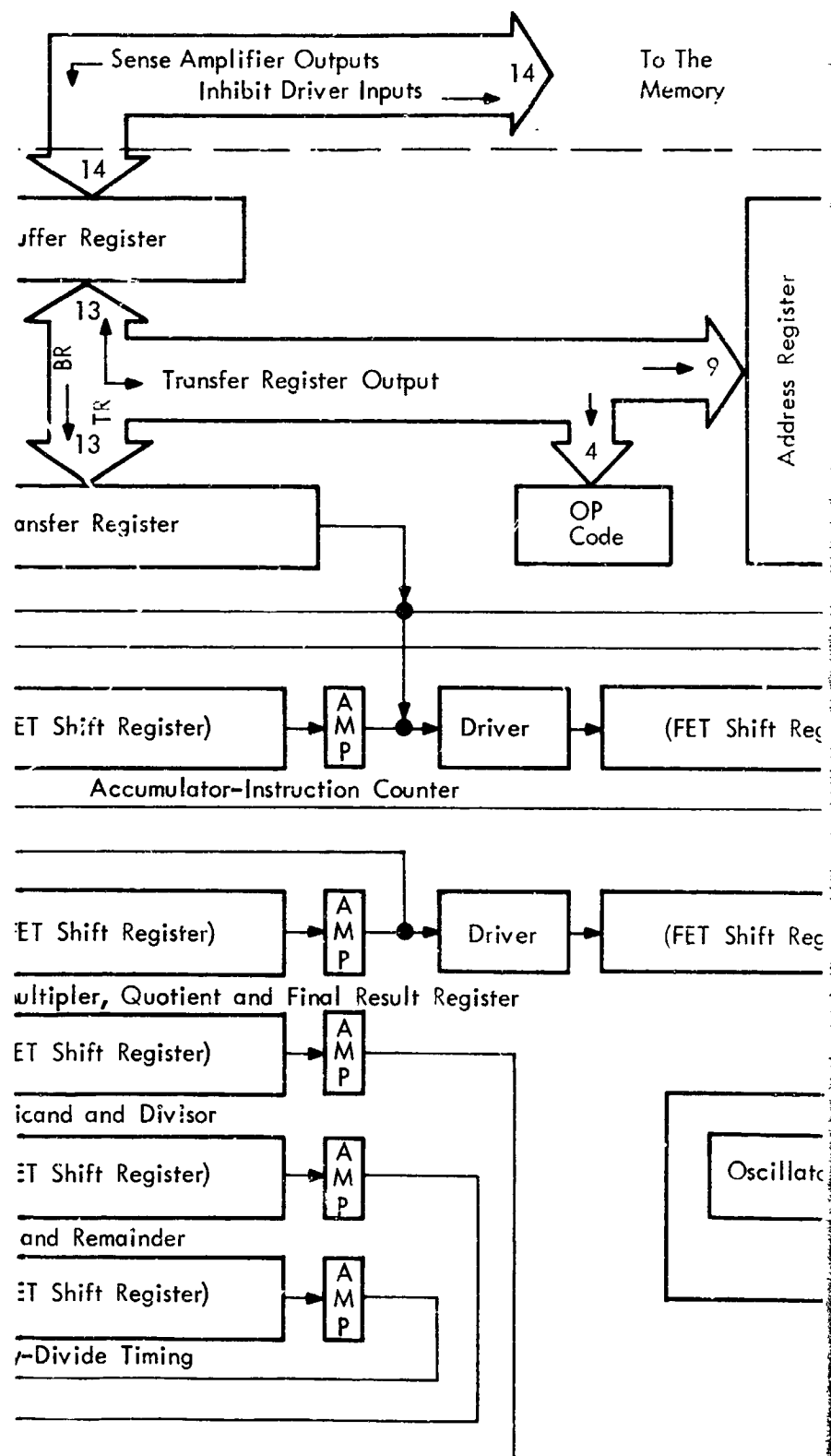
These changes will allow the central computer to perform the computations presently done on the I/O processor or the backup Apollo data adapter. A block diagram of the information flow is shown in Figure 45. A summary of the computer characteristics is given in Table 11.

#### 2.9.2 Data Adapter Description

The organization of the AES data adapter is similar to the Apollo data adapter system described in Section 2.3 except that the I/O processor and bit gate generator were eliminated. The central processor unit bit gate generator will suffice for the Apollo data adapter. Memory-steal was eliminated. The functions which were performed by the processor were assumed by the AES computer except for the task of updating the 32 counting registers. These registers were incorporated as hardware in the form of shifting registers. In addition to the shift registers, each counter has its own add/subtract or shift unit and control logic. To conserve logic, the shift registers utilize the field effect transistor shift registers in which up to 100 bits of storage may be obtained on a single flat pack, which makes the hardware implementation of the counters feasible. The input and real-time counters may be loaded or unloaded by computer command. The output counters can only be loaded by computer command. Data is transferred serially to or from the computer arithmetic element. The static data such as the discrete outputs are stored in latch registers, which are loaded in parallel from the data exchange register (DER). Discrete inputs are transferred in parallel to the DER. This register converts the data from parallel to serial or vice versa for communications with the computer. The real time counter was implemented in hardware as a shift register and the central processor unit interrupt register was increased to 15 bits to allow for time control interrupts.



105  
①



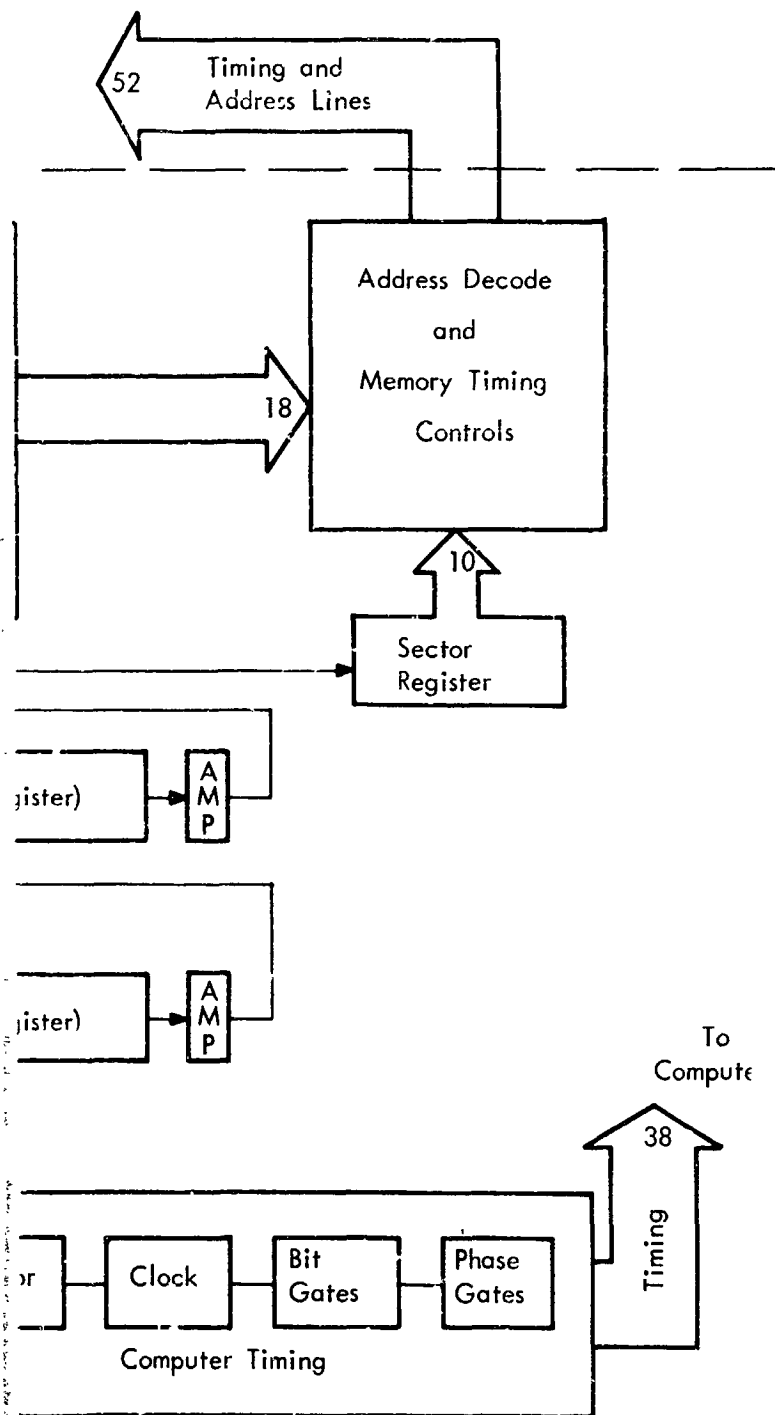


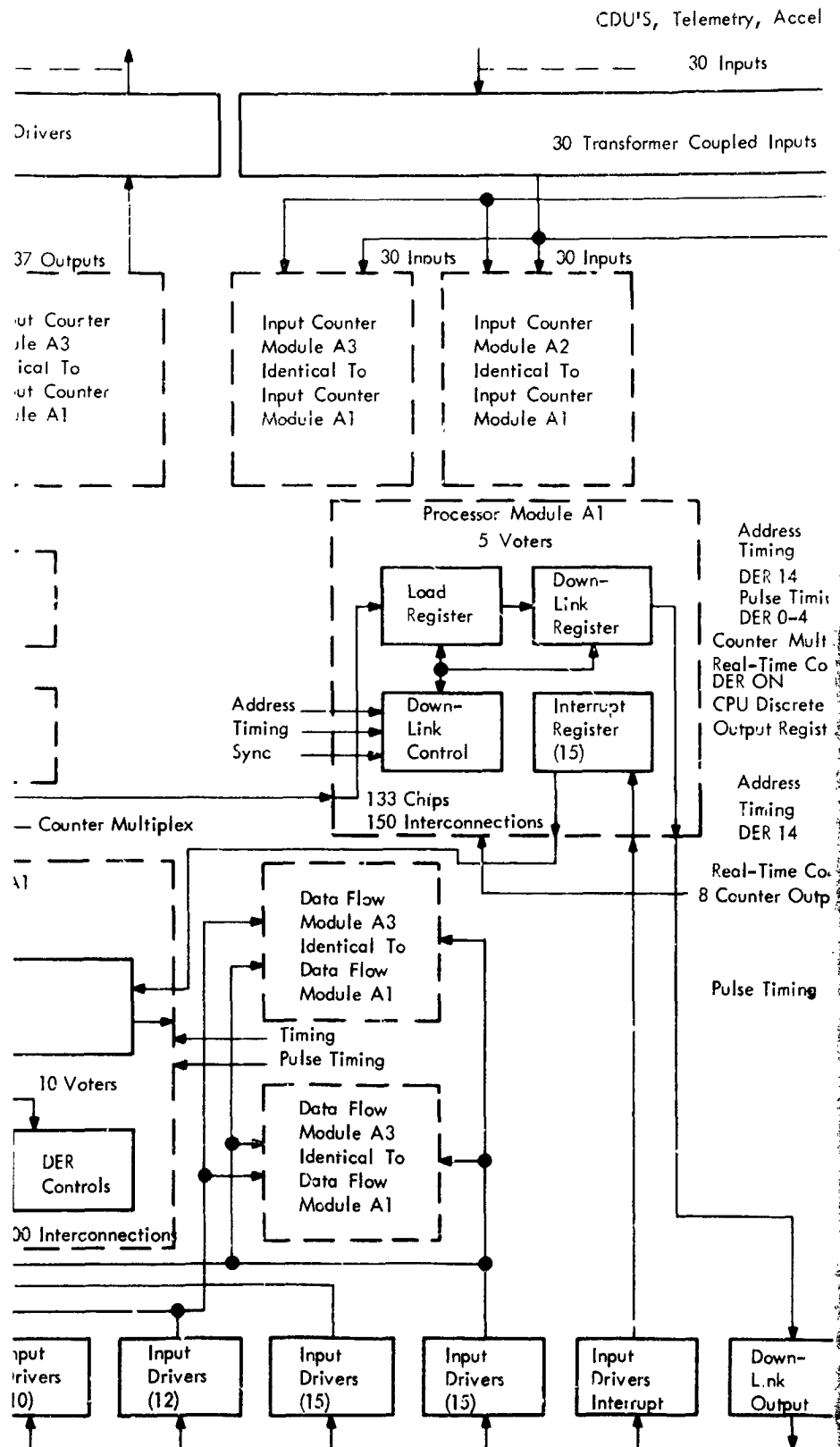
Figure 45. AES Computer Flow Diagram

**TABLE 11 - TMR Computer Characteristics (AES)**

Type	General purpose, stored program, serial, fixed point binary
Clock	2 megobits per second information rate
Speed	Add-subtract and multiply-divide simultaneously
Add	21 $\mu$ s
Multiply	84 $\mu$ s
Divide	168 $\mu$ s
Memory Type	Toroidal magnetic core, random access
Storage Capacity	Three TMR memory modules each having 8192 28-bit words.
Input/Output	External; computer-programmed I/O control. External interrupt provided.
Component Count	47,800 integrated circuit semiconductors and resistors. (4 memory modules)
Reliability	0.9994 probability of success for 90 days
Packaging	21 electronic page assemblies
Weight	69 pounds
Volume (Swept)	1.8 cubic feet
Power	102 watts

The data adapter contains approximately twice as much logic as the computer. This is attributed primarily to the large amount of static storage (latches) required to buffer the input and output signals and control the counting registers. Figure 46 illustrates the basic configuration of the data adapter.





107②

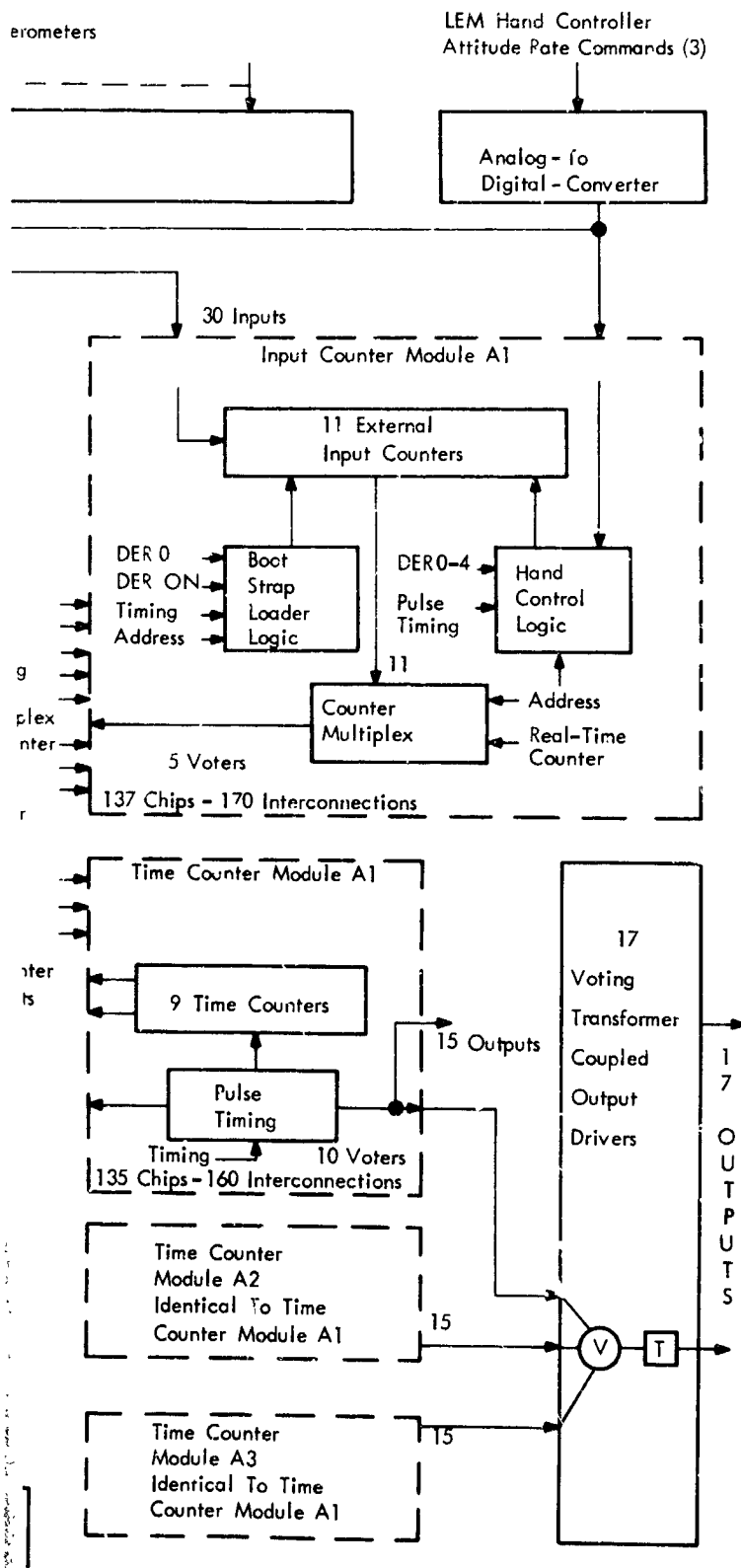


Figure 46. AES Data Adapter Flow Diagram

The partitioning of the data adapter into modules is not as straightforward as in the computer, in that functional areas are not as clearly defined. Also, the use of multiplexor logic to serialize the parallel registers tends to reduce the number of total voters required. This is compensated for in the number of voters required in the interface to the rest of the system. For the system requirements, 121 interface voters are required. These are packaged separately from the six logic modules. Table 12 indicates how the data adapter was partitioned into six modules and the chip or flat pack component count and interconnection requirements. It should be noted that these modules are approximately the size of the computer modules. This is an important consideration if the same packaging philosophy is to be applied to the whole computer-data adapter complex.

The data in Table 12 is based on partitioning the data adapter into six unique modules. It is a possibility that one or two of these modules could be standardized such that only four module types would be required. This standardization would be at the expense of a slight increase in module size and interconnections. The obvious savings are in the spares required to be carried for inflight maintenance.

To preserve the symmetry of the replaceable simplex modules, the data adapter interface voters are packaged separately. These circuits convert the TMR output signals to a single line. Circuit reliability was increased through use of redundant and/or quaded components so as not to degrade the system reliability.

The results of the exploratory (Phase I) and evaluation (Phase II) testing effort described in Section 6 indicated that adequate connector sealing could be maintained during operation and maintenance in the high humidity-zero gravity environment when resorting to over-all unit sealing of the computer or data adapter. The reconfigured computer and data adapter were packaged as a unit for the AES application; the physical organization is illustrated by Figure 47. The individual replaceable modules are shown in individually sealed cans.

### 2.9.3 Reliability Models

A reliability model for the reconfigured computer subsystem was derived and used to compare the reliability characteristics of the reconfigured system with the basic system of Section 2.3. The time models and basic reliability assumptions (such as constant failure rates) are the same as in the reliability model for the basic system although the failure rates of individual component parts are different due to the radically different packaging concept.

**TABLE 12 - Data Adapter Modules**

Module	Functions Contained	Chips*	Interconnections	Voters
1. Output Counter Module	11 Output Counters (includes registers and control) Gyro Logic Radar Counter Logic	140	200	5
2. Input Counter Module	13 Input Counters Counter Multiplexer Hand Control Logic Boot Strap Loader	147	170	5
3. Time Counter Module	9 Time Counters Pulse Timing	155	160	10
4. Data Flow Module	Data Exchange Register Input Multiplexing DER Controls Jet Select Logic	160	200	10
5. Control Module	4 Discrete Output Registers Address Decode Miscellaneous Controls	185	210	30
6. Processor Module	Load Register Downlink Register Downlink Control Interrupt Register	143	150	5
<b>TOTALS</b>		<b>930</b>		<b>65</b>

\* Does not include 242 voter chips associated with output drivers.

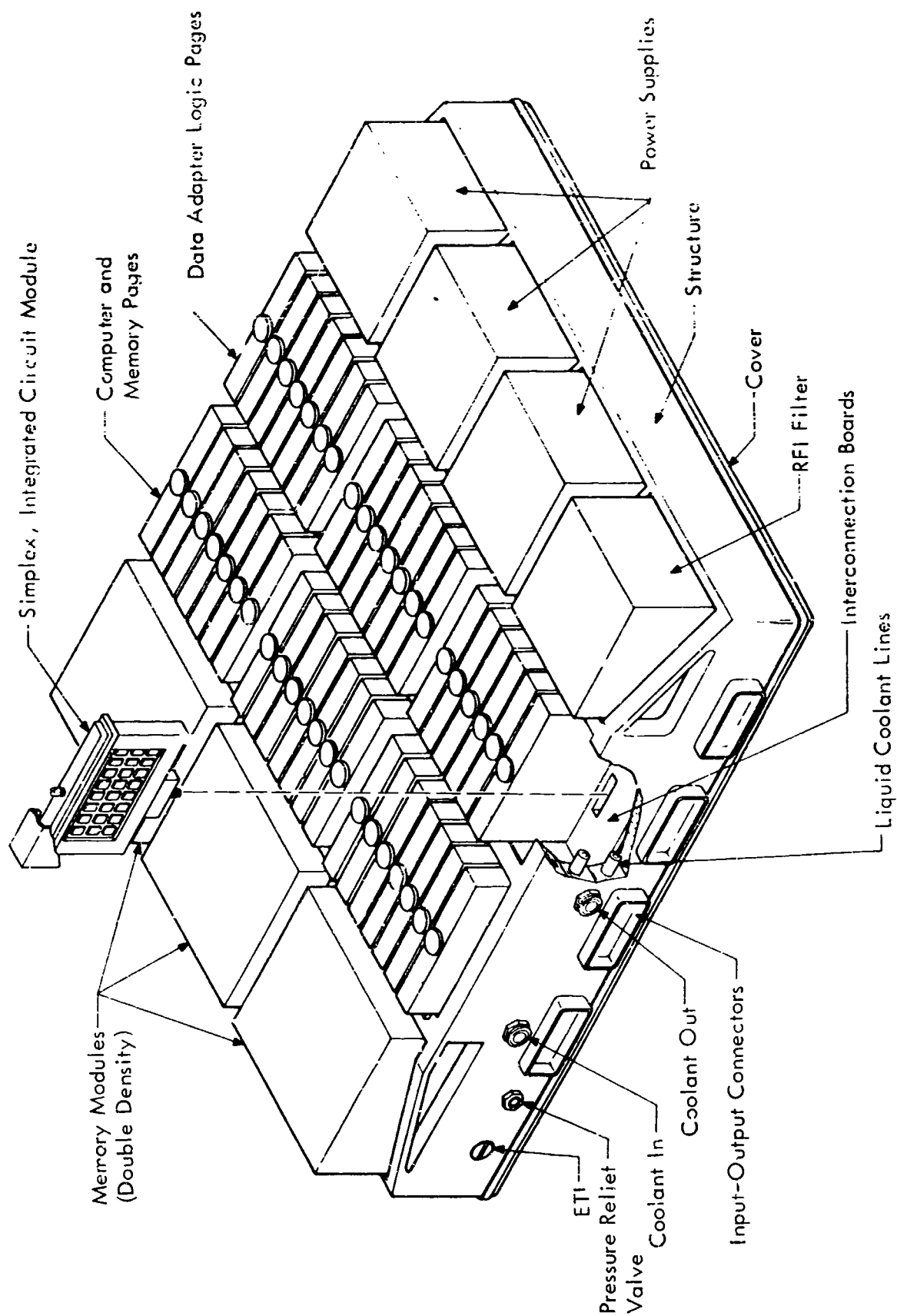


Figure 47. AES Computer Subsystem Package

Since the computer and data adapter operate effectively in series for reliability computations, the model for the computer subsystem is simply

$$R_{ss} = R_{co} R_{da},$$

where  $R_{co}$  is the computer reliability and  $R_{da}$  is the data adapter reliability.

The reorganized computer is composed of a redundant oscillator, TMR logic, and TMR memories:

$$R_{cc} = R_{os} R_{cl} R_{mer}$$

where  $R_{os}$  is the reliability of the oscillator,  $R_{cl}$  is the reliability of the computer logic, and  $R_{mem}$  is the reliability of the memory.

In the gated triplex oscillator, described in Section 2.4, successful operation depends only on the operation of any one of the three simplex oscillators. The reliability model is

$$R_{os} = 1 - (1 - R_o)^3,$$

where  $R_{os}$  is the reliability of the triplex oscillator and  $R_o$  is the reliability of the simplex oscillator.

The computer logic, including the timing generator, is physically divided into three replaceable subassemblies. Hard core (nonreplaceable) hardware is included in the basic frame. The reliability of a TMR module can be expressed mathematically as

$$R_{trio} = 3 (R_{mod})^2 - 2 (R_{mod})^3,$$

where  $R_{mod}$  is the reliability of each simplex module of a TMR module. The reliability module for the computer logic is the product of the reliabilities of the individual logic modules, or

$$R_{cl} = \prod_{i=1}^4 (R_{trio})_i.$$

The reorganized computer uses a TMR memory which operates in a manner similar to the logic and was described in Section 2.5. The model is

$$R_{\text{mem}} = R_m^3 + 3 C_{s2} R_m^2 (1 - R_m) + 3 C_{s3} R_m (1 - R_m)^2 + C_{s3} (1 - R_m)^3,$$

where  $R_m$  is the reliability of one simplex memory module,  $C_{s2}$  is the conditional probability that no identical address bit has failed in the two failed simplex modules, and  $C_{s3}$  is the conditional probability that no same address bit has failed in the three failed simplex modules.

The reorganized data adapter is composed primarily of TMR logic and triplex power supplies:

$$R_{\text{da}} = R_{\text{dal}} R_{\text{ps}},$$

where  $R_{\text{dal}}$  is the reliability of the data adapter logic and  $R_{\text{ps}}$  is the reliability of the power supplies.

The data adapter logic is packaged in six replaceable sub-assemblies, and other hardware (including the input-output circuitry) is mounted on the basic frame. The output drivers and the hard-core hardware were assumed to be TMR as well as the replaceable modules. As in the computer, the reliability of a TMR module can be expressed as

$$R_{\text{trio}} = 3 (R_{\text{mod}})^2 - 2 (R_{\text{mod}})^3.$$

The model for the six replaceable TMR modules and hard core is

$$R_{\text{dal}} = \prod_{i=1}^7 (R_{\text{trio}})_i.$$

A triplex power supply drives both the computer and data adapter. Each supply is composed of three identical converter-regulators with duplex error amplifiers and is connected to drive any or all three of

the TMR channels. Each regulator is protected by isolation diodes. Successful power supply operation is defined in the following ways:

- 1) All regulators (with duplex error amplifiers) work; all isolation circuits work.
- 2) All regulators work; two isolation circuits work and one fails high or low. This can occur in three ways.
- 3) All regulators work; one isolation circuit works and two fail (three ways).
- 4) Two regulators work and one fails low; all isolation circuits work (three ways).
- 5) One regulator works and two fail low; all isolation circuits work (three ways).
- 6) Two regulators work and one fails low; two isolation circuits work and one fails low (three ways).
- 7) One regulator works and two fail low; one isolation circuit works and two fail low (three ways).

The resulting reliability model for a regulator is:

$$\begin{aligned}
 R_{\text{reg}} = & (R_S R_I)^3 + 3 R_S^3 R_I^2 (1 - R_I) \\
 & + 3 R_S^3 R_I (1 - R_I)^2 \\
 & + 3 R_S^2 P_{\text{SFL}} R_I^3 \\
 & + 3 R_S P_{\text{SFL}}^2 R_I^3 \\
 & + 3 R_S^2 P_{\text{SFL}} R_I^2 P_{\text{IFL}} \\
 & + 3 R_S P_{\text{SFL}}^2 R_I P_{\text{IFL}}^2,
 \end{aligned}$$

where  $R_{reg}$  is the triplex reliability of one regulator,  $R_S$  is the reliability of one converter-regulator with duplex error amplifiers,  $R_I$  is the reliability of one isolation diode,  $P_{SFL}$  is the probability that a converter-regulator fails low, and  $P_{IFL}$  is the probability that an isolation diode fails low. Since there are six regulators in the power supply, the reliability of the power supply is given by

$$R_{ps} = \prod_{i=1}^6 (R_{reg})_i.$$

#### 2.9.4 Reliability Estimates

Simulations were performed to derive the reliability estimates for the reorganized computer and data adapter. These reliability estimates are summarized in Table 13 for the time-critical phases and for the mission. The latter is estimated for duty cycles of 100, 50, and 25 percent and for zero and non-zero standby failure rates. The mission reliability figures represent the basic long-term reliability of the equipment. The sparing requirements to raise these figures to the required 0.9994 mission reliability are described in Section 2.9.5. Note that the required computer subsystem reliability of 0.999999 for the critical mission phases has been achieved by the basic TMR configuration without resorting to the TMR/simplex switching mode. The instrumentation of this TMR/simplex mode would provide significant improvement even though the study goal has been met without it.

Table 14 summarizes these reliability estimates of the AES equipment in the TMR/simplex mode. These estimates represent only the degree of reliability attainable with this mode of operation but do not account for the possible reliability degradation provided by the switching mechanism required to accomplish this.

#### 2.9.5 Sparing Considerations

In Section 2.9.4 reliability estimates of the AES computer/data adapter system were presented. Mission reliabilities for the various types of missions ranged from about 0.9699 to 0.9979, all which fall below the required 0.9994 for the AES mission. In order to meet the required reliability, inflight maintenance in the form of spare sub-assemblies had to be implemented. The problem then was one of

TABLE 13 - Reliability Estimates (AES System - TMR Mode)

Element	Critical Phase	100%	Non-op $\lambda > 0$		Non-op $\lambda = 0$	
			50%	25%	50%	25%
Computer	0.9999994	0.978717	0.989052	0.993031	0.994346	0.998542
Oscillator	$\approx 1.000$	$\approx 1.000$	$\approx 1.000$	$\approx 1.000$	$\approx 1.000$	$\approx 1.000$
Logic	0.99999999	0.999647	0.999822	0.999888	0.999909	0.9999765
Memory	0.9999994	0.979063	0.989228	0.993142	0.994437	0.998566
Data Adapter	0.9999997	0.991132	0.995442	0.997092	0.997639	0.999372
Logic		0.999389	0.999697	0.999808	0.999845	0.999959
Input/Output		0.991728	0.995743	0.997282	0.997793	0.999412
Power Supply	0.99999992	0.999900	0.999951	0.999975	0.999976	0.999995
System	0.9999991	0.969941	0.984496	0.990118	0.991976	0.997911

TABLE 14 - Reliability Estimates (AES System - TMR/Simplex Mode)

Element	Critical Phase	100%	Non-op $\lambda > 0$		Non-op $\lambda = 0$	
			50%	25%	50%	25%
Computer	0.99999946	0.981708	0.990500	0.993921	0.995062	0.998716
Oscillator	$\approx 1.000$	$\approx 1.000$	$\approx 1.000$	$\approx 1.000$	$\approx 1.000$	$\approx 1.000$
Logic	0.99999999	0.999824	0.999911	0.999944	0.999955	0.999988
Memory	0.99999947	0.981882	0.990588	0.993977	0.995107	0.998728
Data Adapter	0.99999988	0.995488	0.997693	0.998532	0.998809	0.999685
Logic	0.99999999					
Input/Output	0.99999925	0.995788	0.997844	0.998627	0.998886	0.999705
Power Supply	0.99999997	0.999900	0.999952	0.999975	0.999976	0.999995
System	0.99999927	0.977181	0.988167	0.992437	0.993854	0.998397

determining the optimum spares inventory required to achieve the desired reliability. Optimization of this inventory for this study was based on the criteria

$$R_{wi} = \frac{\Delta R_i \cdot P_{ai}}{W_i},$$

where

$R_{wi}$  = Weighted ranking criteria for  $i^{\text{th}}$  spare

$\Delta R_i$  = Increase in system reliability provided by  $i^{\text{th}}$  spare

$P_{ai}$  = Probability of detecting a failure in the  $i^{\text{th}}$  module

$W_i$  = Weight of the  $i^{\text{th}}$  spare

An ordered list of spares was generated which provides the greatest increase in system reliability for the added weight of the spare.

Table 15 is a list of subassemblies in the system which are available for sparing.

Tables 16 through 20 are lists of spares selected according to this criteria. Each of these lists represents those spares required for a mission of the specified equipment duty cycle and nonoperating failure rate condition. Each list consists of two parts: 1) a list of the subassemblies available for sparing the system and 2) the list showing the order and quantity of each subassembly selected, the resultant non-critical phase system reliability, and the cumulative weight.

Table 21 is a summary of the improved reliability showing the combined reliability of the launch, orbit inject, and orbit adjust phases; the orbit phase reliability before and after sparing; the weight of spares required to obtain this reliability; and the total mission system reliability just prior to re-entry.

This configuration includes the possibility that only two of the three modules of each TMR trio will survive until the end of the orbit phase. Therefore, a full TMR configuration will not exist just prior to re-entry. Without the full TMR capability, the critical re-entry phase will not meet the critical phase reliability requirements.

If re-entry must be considered as a critical phase and must meet that requirement, it will be necessary to carry an additional complement of spares in order to restore the system to its full redundant capability just prior to re-entry. This requires one each of the logic pages and memory modules and two power supply modules, a total of 16.8 pounds, in addition to the spares required to achieve the mission requirement.

**TABLE 15 - List of Available Spares**

	Spare Number	Subassembly Name	Weight (lbs)
Computer	1	Arithmetic	0.43
	2	Address Register	0.43
	3	Control/Timing	0.43
Memory	4	Memory Module	4.50
Data Adapter	5	Output Counter	0.43
	6	Input Counter	0.43
	7	Time Counter	0.43
	8	Data Flow	0.43
	9	Control	0.43
	10	Processor	0.43
	11	Input/Output	0.43
Power Supply	12	Power Supply Module	4.00

If re-entry is not a critical phase, the system may be in a "two parallel" configuration at the end of the orbit phase, that is, only two simplex modules of each trio may be operating. If the TMR/simplex switching modification is available, one each of these parallel modules may be switched out and the entire system operated simplex during re-entry.

Table 22 shows the unit and system reliabilities for the re-entry phase for each of these three equipment configurations.

Table 23 then gives the total mission reliability for the AES system with the three re-entry configurations. Only when the system operates at its full redundant capability during re-entry will the total mission reliability requirement of 0.9994 be achieved.

**TABLE 16 - On-board Spares - 100-Percent Duty Cycle**

Duty Cycle		100%		
Spare Number	Subassembly Name	Delta Reliability	Cumulative Weight (lbs)	System Reliability
11	Input/Output	0.00737480	0.43	0.97749496
4	Memory Module	0.01608645	4.93	0.99358141
11	Input/Output	0.00071146	5.36	0.99429286
4	Memory Module	0.00443837	9.86	0.99873123
1	Arithmetic	0.00012259	10.29	0.99885383
9	Control	0.00012093	10.72	0.99897476
3	Control Timing	0.00011069	11.15	0.99908544
8	Data Flow	0.00009657	11.58	0.99918202
7	Time Counter	0.00009165	12.01	0.99927367
6	Input Counter	0.00008464	12.44	0.99935830
10	Processor	0.00008128	12.87	0.99943958
12.87 Pounds of spares required.				

**TABLE 17 - On-board Spares - 50-Percent Duty Cycle,  
Non-op Failure Rate >0**

Duty Cycle		50%		
Non-op failure rate		>0		
Spare Number	Subassembly Name	Delta Reliability	Cumulative Weight (lbs)	System Reliability
11	Input/Output	0.00388689	0.43	0.98851638
4	Memory Module	0.00894830	4.93	0.99746468
11	Input/Output	0.00024814	5.36	0.99771282
4	Memory Module	0.00171687	9.86	0.99942970
9.86 Pounds of spares required.				

**TABLE 18 — On-board Spares - 25-Percent Duty Cycle,  
Non-op Failure Rate >0**

Duty Cycle		25%		
Non-op failure rate		>0		
Spare Number	Subassembly Name	Delta Reliability	Cumulative Weight (lbs)	System Reliability
11	Input/Output	0.00249953	0.43	0.93272476
4	Memory Module	0.00592437	4.93	0.99864914
11	Input/Output	0.00012162	5.36	0.99877076
4	Memory Module	0.00089125	9.86	0.99936200
9.86 Pounds of spares required.				

**TABLE 19 — On-board Spares - 50-Percent Duty Cycle,  
Non-op Failure Rate = 0**

Duty Cycle		50%		
Non-op failure rate		= 0		
Spare Number	Subassembly Name	Delta Reliability	Cumulative Weight (lbs)	System Reliability
11	Input/Output	0.00203302	0.43	0.99410621
4	Memory Module	0.00487773	4.93	0.99898394
11	Input/Output	0.00008739	5.36	0.99907133
4	Memory Module	0.00065684	9.56	0.99972817
9.86 Pounds of spares required.				

TABLE 20 — On-board Spares - 25-Percent Duty Cycle,  
Non-op Failure Rate = 0

Duty Cycle		25%		
Non-op failure rate		= 0		
Spare Number	Subassembly Name	Delta Reliability	Cumulative Weight (lbs)	System Reliability
11	Input/Output	0.00053165	0.43	0.99949373
4	Memory Module	0.00140191	4.93	0.99989564
4.93 Pounds of spares required.				

TABLE 21 — Reliability Improvement Due to Sparing

Mission Duty Cycle	Spare Weight (lbs)	Orbit Phase (Before Sparing)	Orbit Phase (After Sparing)	Mission Reliability (Prior to Re-entry)
100	12.87	0.970120	0.999439	0.999437
50*	9.86	0.984629	0.999429	0.999427
25*	9.86	0.990225	0.999662	0.999660
50**	0.86	0.992073	0.999728	0.999726
25**	4.93	0.997962	0.999635	0.999893
* Non-op $\lambda > 0$ ** Non-op $\lambda = 0$				
Pre-orbit Reliability = 0.9999981				

**TABLE 22 — AES System Reliability - Re-entry Phase**

Element	System Configuration		
	TMR	Two Parallel	Simplex
Computer	0.999999996	0.9998638	0.999 244
Data Adapter	0.999999908	0.99943172	0.9997158
Memory	0.999999763	0.99941414	0.9996240
Power Supply	0.999999999	0.99977775	0.99977775
System	0.999999667	0.9984317	0.99904227

**TABLE 23 — AES Mission Reliability**

Mission Duty Cycle	Total Mission Reliability		
	TMR	Two Parallel	Simplex
100%	0.999436	0.997931	0.998479
50%*	0.999426	0.997921	0.998469
25%*	0.999659	0.998153	0.998702
50%**	0.999725	0.998219	0.998768
25%**	0.999892	0.998386	0.998935
* Non-op $\lambda > 0$ ** Non-op $\lambda = 0$			

In Section 2.8, a concept of the ultimate reliability of the TMR/simplex mode was discussed. This mode of operation is actually a sparing situation because the switched-out module may ultimately be used as a switchable spare.

Table 24 presents the reliability estimates of the AES system with this capability in the noncritical coast phase only.

TABLE 24 - AES System Reliability - Switchable Space Mode

Element	100%	Non-op $\lambda > 0$		Non-op $\lambda = 0$	
		50%	25%	50%	25%
Computer	0.9999993	0.99999997	0.9999998	0.999999991	0.99999998
Memory	0.99859	0.99926	0.99974	0.99981	0.999974
Data Adapter	0.999851	0.999946	0.999973	0.999980	0.999997
Power Supply	0.99990	0.999951	0.999975	0.999976	0.999995
System	0.99830	0.99915	0.99969	0.99976	0.999966

The system must be in a TMR configuration for the critical re-entry phase to meet its reliability requirement. With the switchable spare capability, the entire system may be operating simplex at the end of the coast phase. To restore it to a TMR configuration would require two additional subassemblies of each type, a total of 25.6 pounds. If the system is not restored to a TMR configuration, it may operate simplex throughout the re-entry phase.

Table 25 shows the system mission reliability with the two re-entry configurations. Only with the TMR configuration during re-entry is the mission reliability requirement achieved, but this can be accomplished more economically by selecting a more optimum stock of spares.

TABLE 25 - AES System Reliability - Total Mission

Re-entry Configuration	100%	Non-op $\lambda > 0$		Non-op $\lambda = 0$	
		50%	25%	50%	25%
TMR	0.998337	0.999154	0.999685	0.999763	0.99996
Simplex	0.997381	0.998197	0.998728	0.998803	0.99900

### 2.9.6 Error Detection and Fault Isolation

Simulations were performed on the basic computer using the IBM 7090 logic simulator to determine the error detection and fault isolation capabilities of the computer. Since Saturn-V test programs were found to be adequate for simulation purposes, the appreciable test programming effort which was visualized at the start of the study was not required. The test programs were used to operate the logic simulator which simulated selected failure conditions and produced error symptoms.

Error detection is accomplished in the Saturn-V computer by means of disagreement detectors which sense a difference in the three channels feeding a voter. These disagreement detectors consist of three-way exclusive OR circuits. Since the Saturn-V computer contains approximately 200 disagreement detectors, the outputs of groups of detectors are "OR'd together to provide 13 signals to an error monitor register in the data adapter. The inputs to the detectors are clocked to allow time for the input signals to reach steady-state conditions before sampling.

The logic simulation of the basic computer confirmed earlier simulation results with the Saturn-V computer that indicated a 99-percent detection efficiency based on the disagreement detectors. That is, once the logic was screened for undetected failures involving redundant logic elements or circuits which were included in the computer design to conserve power or to ensure against marginal conditions, 99-percent of the component failures injected into the simulator were detected by the disagreement detectors when the simulator was being operated by a standard operation code exerciser test program. In fact, extensive propagation of errors through the computer tended to be sensed by many detectors even though these detectors were not directly associated with the logic containing the fault, thus masking the source of the error by overdetection.

Although the computer was judged on the basis of the logic simulation results to possess adequate error detection capabilities, fault isolation under AES mission conditions was judged inadequate in several areas. An assumption of the study was that error detection and fault isolation should necessarily be automatic. Since the disagreement detectors indicate only that there is a difference in the information contained in the three channels and not which channel disagrees with the other two, channel or module switching would have to be performed by the astronaut to isolate the error to a replaceable simplex module. Also, since the voters existed at the module interfaces and since the

detectors are positioned at the voter inputs, only clever analysis of the disagreement patterns by the astronaut could differentiate between a voter failure in one module and a logic failure in the module following the suspected voter.

Overdetection occurs by propagation of errors in time as well as in circuitry. Saturn-V disagreement detectors are clocked every like clock time (for example, any one disagreement detector may be clocked every x-time, another every y-time, etc.). As a result, detectors are sensing for disagreements between the simplex modules of a TMR trio even at times when those modules are not being used by the program, making any diagnostic correlation between the detectors and program very difficult.

The "OR-ing" network which reduced the 200 disagreement signals to 13 error monitor signals was found to need modification to improve the fault isolation capabilities of the computer. Several identical disagreement patterns resulted from different component failures which could have been isolated if the respective detector outputs had been routed or clocked in different times to different positions in the error monitor register.

For example, Table 26 shows the error patterns of some voter failures which gave the same diagnostic error symptoms, although the failure signals were located in different modules.

To unscramble identical error-pattern symptoms, simulation experiments were performed. Errors were injected into the simulation program, and the error propagation was noted. This was done by observing the responses of the disagreement detectors. From these results, optimum timing and placement of some disagreement detectors (DD) could be determined.

An example of this optimization is shown in Table 27. In the first failure, symptoms could be unscrambled by clocking the status of the TRSN disagreement detector into the error monitor register at either instruction CLA 776 or STO 776. CLA 776 would pinpoint the error to the RDV signal net, and STO 776 would indicate that the MD2V signal net has failed.

In the second example, the CDS and SYLO disagreement detector would be removed from the OR EP5 and EP9 position and assigned to a new error monitor position. This would permit isolation of the STONV and RUNNV signal net failures. Similar results can be obtained for the other conflicting symptom conditions. A trade-off would have to be made in cost of hardware to obtain this failure isolation capability.

TABLE 26 — Disagreement Patterns

Failure No.	Signal Name	Module Location	Error Pattern of Detectors											
			7	11	5	1	2	3	4	6	9	10	12	8
1	RDV MD2V	7		X	X									
		4		X	X									
2	RUNNV STONV	7		X	X						X	X		
		4		X	X						X	X		
3	TRSN OP4N PIO	2				X			X					
		5				X			X					
		5				X			X					
4	VO4V RUNV	4				X		X						
		5				X		X						
5	A9V TR10V	6								X				
		2								X				
6	TBCV OP3NV Q8	Timing				X		X	X					
		5				X		X	X					
		4				X		X	X					

## 2.10 Transient Protection

Considerable effort was expended to ensure adequate protection of the computer memory from voltage transients of external origin. The nature of the Gemini computer memory alterations was investigated to determine if these same types of alterations can occur in the Saturn-V or AES computers. (Most of the Gemini computer memory alterations appeared to result from the alteration of address information. The addition or deletion of bits resulted from voltage transients between the computer chassis and signal ground.)

Methods of preventing memory alterations due to address modifications were investigated. Consideration was given to the magnitude of this problem in relationship to simple hardware failures which can be overcome by redundancy. Possible solutions to the transient problem involved additional selective redundancy, separation of channels to the extent practical, and improved circuitry.

TABLE 27 — Diagnostic Listings

Instruction CLA776, Step 001							
Failure No.	Signal Name	Failure State	First Detection Phase, Bit, Clock	Error Pattern	Disagreement Detector	Optimum Time	Optimum Place
1	RDV	0	B3Z	11	TR1, TR3	X	
			B4W	11	TR2, TR4		
			F4Z	11	TR5		
			B5W	11	TR6, TR7		
			B5Z	11	TR8		
			B6W	11	TR9		
			B8X	5	TR10		
			B8Z	5	TR11		
			B9W	5	TR12		
			B10X	5	TR13		
			B11W	5	TRSN		
	RDV	1	C2Z	5, 11	TR8, TR11		
			C3W	5, 11	TR2, TR7, TR9		
			C3Z	11	TR3		
			C4X	5	TR13		
			C5W	5, 11	TR4, TRSN		

TABLE 27 -- Diagnostic Listings (cont)

Instruction CLA776, Step 001						
Failure No.	Signal Name	Failure State	First Detection Phase, Bit, Clock	Error Pattern	Disagreement Detector	Optimum Time Optimum Place
			C5X	5	TR10	
			C5Z	11	TR5	
			C6W	11	TR6	
Instruction STO776, Step 000						
1	MD2V	0	B9Z	11	TR1	
			B11W	11	TR2	
			B11Z	11	TR3	
			B13W	11	TR4	
			B13Z	11	TR5	
			B14W	11	TR6	
			C2W	11	TR7	
			C2Z	11	TR8	
			C3W	11	TR9	
			C5X	5	TR10	
			C5Z	5	TR11	
			C6W	5	TR12	

TABLE 27 -- Diagnostic Listings (cont)

Instruction STO776, Step 000							
Failure No.	Signal Name	Failure State	First Detection Phase, Bit, Clock	Error Pattern	Disagreement Detector	Optimum Time	Optimum Place
1	MD2V	1	C7X	5	TR13	X	
			C8W	5	TRSN		
			B2Z	11	TR1		
			B4W	11	TR2		
			B4Z	11	TR3		
			B3W	11	TR4		
			B6Z	11	TR5		
			B7W	11	TR6		
			B9W	11	TR7		
			E9Z	11	TR8		
1	MD2V	1	B10W	11	TR9	X	
			B12X	5	TR10		
			B12Z	5	TR11		
			B13W	5	TR12		
			B14X	5	TR13		
			C01W	5	TRSN		

TABLE 27 — Diagnostic Listings (cont)

Instruction STO776, Step 000						
Failure No.	Signal Name	Failure State	First Detection Phase, Bit, Clock	Error Pattern	Disagreement Detector	Optimum Time Optimum Place
2	RUNNV	1	A7Z	9	RD, INHBS	
			A8Y	10	MOSYNC	
			A4W	11	TR4	
			A4Z	11	TR5	
			A5W	11	TR6	
			A7W	11	TR7	
			A7Z	11	TR8	
			A3Z	11	TR13	
			A4W	11	TR2	
			A5Z	11	TR1	
			A4X	5	TR10	
			A4Z	5	TR11	
			A5W	5, 11	TR9, TR12	
			A6X	5	TR13	
			A7W	5, 11	TRSN	
2	STONV	0	A7Z	9	RD, INHBS	
			A14Y	10	MOSYNC	

TABLE 2/ - Diagnostic Listings (cont)

Instruction STO776, Step 000							
Failure No.	Signal Name	Failure State	First Detection Phase, Bit, Clock	Error Pattern	Disagreement Detector	Optimum Time	Optimum Place
2	STONV	1	B7X	9	SYLO, SYLIN		
			B2W	5, 11	TR6, TR12		
			B2Z	5, 11	TR1, TR11		
			B3W	11	TR2, TR9		
			B3X	5	TR10, TR13		
			B3Z	11	TR3		
			B4W	5	TRSN		
			B14X	5	CDS		X
			A13Z	9	RD, IMHBS		
			A14Y	10	MOSYNC		
			B7X	9	SYLO, SYLIN		X
			B11W	11	TR1		
			B11Z	11	TR2		
			B13W	11	TR3		
			B13Z	11	TR4		
			B14W	11	TR5		
				11	TR6		

TABLE 27 — Diagnostic Listings (cont)

Instruction STO776, Step 000							
Failure No.	Signal Name	Failure State	First Detection Phase, Bit, Clock	Error Pattern	Disagreement Detector	Optimum Time	Optimum Place
			C2W	11	TR7		
			C2Z	11	TR8		
			C3W	11	TR9		
			C5X	5	TR10		

### 2.10.1 Gemini Experience

The results of the transient susceptibility tests of the Gemini computer performed over the last few months were reviewed to determine their applicability to the AES-EPO computer organization. The most transient-sensitive areas of the Gemini computer (next to jitter in the cross-over detectors) were found to be the memory sense lines and the output lines of the delay line sense amplifiers. Since the memory sense lines operate with signal levels in the order of 10 millivolts, low-level noise introduced on these lines will cause zeros to be read as ones. The delay line drive and sense amplifiers are cabled to the remainder of computer logic (rather than connected by multi-layer board lines) and are therefore more noise sensitive than other logic circuits of essentially the same noise rejection levels.

The specific types of errors encountered during the transient susceptibility tests included cross-over detectors, accumulator shift, add and subtract, multiply, RDR, DAS, DCS, modified diagnostic program, and I/O processor failures. Although the shift, add, subtract, and multiply errors appeared to be of different types, these errors were found to have a common source. In each case, the errors were the result of transient noise coupled into the memory sense lines on the panel interconnecting the memory multiplex circuits. The noise resulted in the incorrect reading of memory data.

Because of the low signal levels in these areas, it was not feasible to measure the magnitude of the noise. The output of the memory sense amplifiers was observed while injecting transient noise into the cable test loop. Errors occurred mainly in memory locations having the most zeros.

Analysis of the Gemini data indicates that the following features should be incorporated into the AES design to decrease the susceptibility of the memories to voltage transients:

- 1) TMR organization,
- 2) Improved layout of the multilayer interconnection board (MIB) sense lines
- 3) Limited bandwidth sense amplifiers
- 4) Alternately strobed memories
- 5) Isolated memory grounding.

### 2.10.2 TMR Organization

Whether or not a TMR organization per se will decrease the transient susceptibility of the computer subsystem has not been determined. Unless the transient manifests itself as a local phenomenon within the computer, the TMR organization will be no less susceptible than a simplex organization. The Gemini tests resulted in somewhat conflicting results regarding the propagation characteristics of externally generated voltage transients. Isolating the computer chassis by removing ground shields in the cable apparently decreased the threshold of the transient noise applied to the chassis relative to power and reference ground by altering the number of return paths and thereby changing the distribution and concentration of currents flowing in the chassis. On the other hand, changes in the point of contact of the noise generator probe on the computer chassis seemed to have no effect on the threshold level. An investigation of the propagation characteristics of externally generated voltage transients in computer organizations should be performed but is beyond the scope of this study. The assumption is therefore made that additional transient protection must be designed into the AES-EPO computer organization, especially in the area of TMR memories.

### 2.10.3 Sense System

Tests at IBM have indicated that the rise time of a voltage transient is probably the most critical parameter in defining the transient susceptibility of a digital machine - even more significant than voltage levels or durations. Rise times of the order of a few nanoseconds at relatively low voltage levels have resulted in computer failures in the laboratory while longer rise times at substantially higher voltage levels have been tolerated. Unfortunately, transients with rise times of 50 nanoseconds and less are apparently a common occurrence in operational systems.

The relatively poor high frequency common mode rejection of the Gemini memory sense system could be improved in the AES computer organization by careful MIB layout of the memory sense lines. Further improvement in high frequency common mode rejection probably can be attained, however, by reducing the bandwidth of the sense system to a minimum allowed by strobe margins. It was found in the Gemini testing that an optimum sense system bandwidth exists such that maximum strobe margins are obtained. This maximum strobe margin at a specific bandwidth is due to the fact that zeros read from memory have higher frequency components than the ones. The rate of change of the area

of a zero therefore decreases at a faster rate than the area of a one as the bandwidth of the sense system is reduced. The optimum bandwidth of the memory in Gemini was found to be approximately 1 megacycle for maximum strobe margins.

#### 2.10.4 Memory Strobing

A class of voltage transients which appears to be common in digital systems is a high frequency (20 megacycles or greater) burst lasting less than 1 microsecond. Assuming that these bursts are coupled into all three TMR channels and that they are not sufficiently suppressed by the limited bandwidth of the memory sensing system, memory errors will be generated. If each simplex memory of the TMR configuration is strobed at consecutive time intervals rather than simultaneously, however, the noise burst will affect only one channel of the memory, and no system error will occur. The data from the alternately strobed memories could be stored in individual buffers with synchronized outputs.

This instrumentation would require the reinstatement of the memory buffer registers (eliminated in the reorganized computer) and a slight decrease in computing speed. The feasibility of the approach, the scope of instrumentation required, and the resulting transient protection effectiveness should be further investigated.

#### 2.10.5 Isolated Grounds

Isolated channel grounds in transient susceptible areas such as the memory would reduce the probability of system error due to an externally generated voltage transient. The three channel grounds would be routed independently to the computer memory from the common ground plane in the data adapter. Isolated channel grounds in a TMR memory would require pulse transformers in the output lines of the voters in the logic module driving the memory module and differential amplifiers in the channel inputs to the output voters of the memory module.

### 3.0 ERROR DETECTION AND DIAGNOSIS

The Saturn-V computer and a redundant version of the Apollo backup data adapter were examined to determine the required organization to allow efficient error detection and failure isolation for inflight maintenance in an AES-EPO mission. The machine organization was required to be such as to allow failure isolation down to each separate channel, module, voter, or replaceable spare. Failure detection efficiency was required to be sufficient to assure that all channels are operative prior to a critical phase of the mission. Feasibility of computer programs to isolate these failures was investigated as well as the organization of disagreement detector nets.

#### 3.1 Approach

The Saturn-V computer and data adapter use majority voting circuits which provide correct system operation even when several randomly located failures exist in the hardware. Correct operation is possible even if two failures exist in the same functional area of any two channels if the logic feeding the voters has failed to opposite states. Correct operation is also possible if two or more failures exist in the same functional area of the three channels if the failure effects are non-continuous and occur at different times or if the failures exist at different points in the data flow (such as different positions in a shift register) with voting between the failed positions. Although these TMR error masking characteristics are conducive to achieving very high reliabilities, the problem of error detection and fault isolation is increased by the very error masking features for which TMR was invented.

Failure conditions in the Saturn-V computer and data adapter are detected by means of disagreement detector circuits located primarily at voter inputs. Failure isolation is accomplished by means of disagreement detector signal data, channel switching, module switching, and data analysis. Special test programs are required to accomplish the task of error detection and fault isolation. The functions of voting and disagreement detection are shown in Figure 48.

Channel switching in the Saturn-V computer and data adapter provides the capability of switching the TMR equipment into a simplex operating mode by forcing two of the three channels into opposing logic levels and thereby causing the third channel to control operation. Since any channel may be selected as the operating channel, three simplex modes are provided. Channel switching may be performed in the laboratory or on the launch pad.

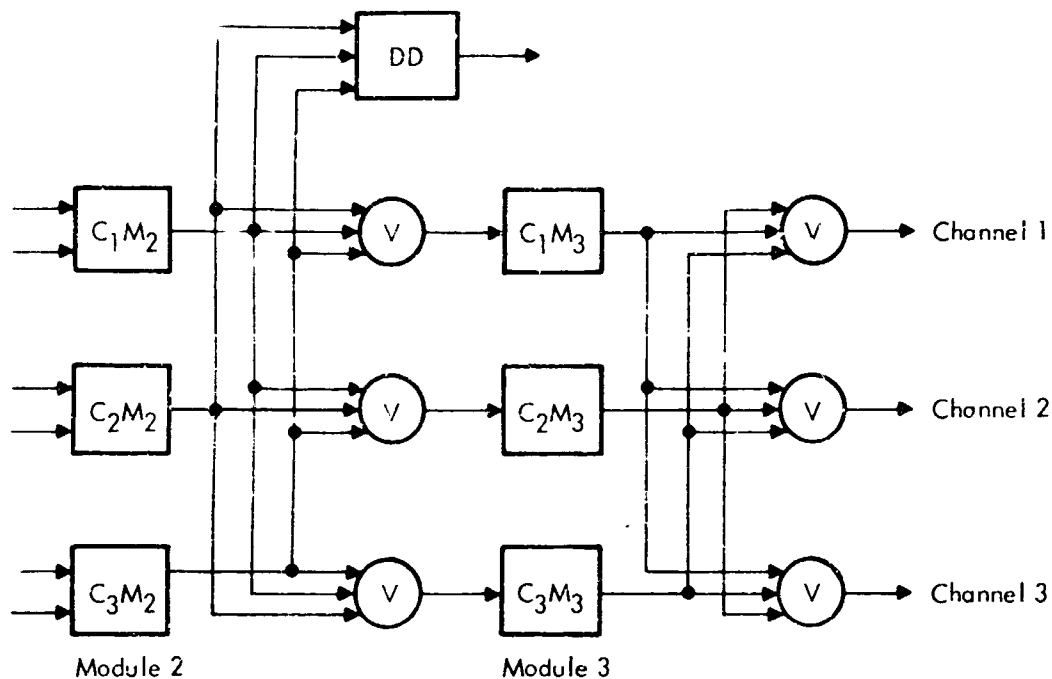


Figure 48. Voting and Disagreement Detection

Module switching in the Saturn-V computer provides simplex operating capability as in channel switching, but the operating channel can be formed by selecting modules from two or more of the three physical channels. The data path can therefore be made to jump between channels as the data progresses from module to module as shown by the solid path in Figure 49. Module switching may be performed only in the laboratory.

The approach to solving the problems of error detection and fault isolation to a replaceable module level was primarily by means of built-in test and switching circuits in this study. Test and diagnostic programs were a secondary consideration meant to fill any gaps in the test functions left by the hardware approach. Simulation of the computer configurations on an IBM 7090 computer was the primary analytic tool.

### 3.1.1 Hardware

Any computer development program includes a set of hardware/software trade-off studies to determine the optimum characteristics for the particular application. In a development program for an advanced AES

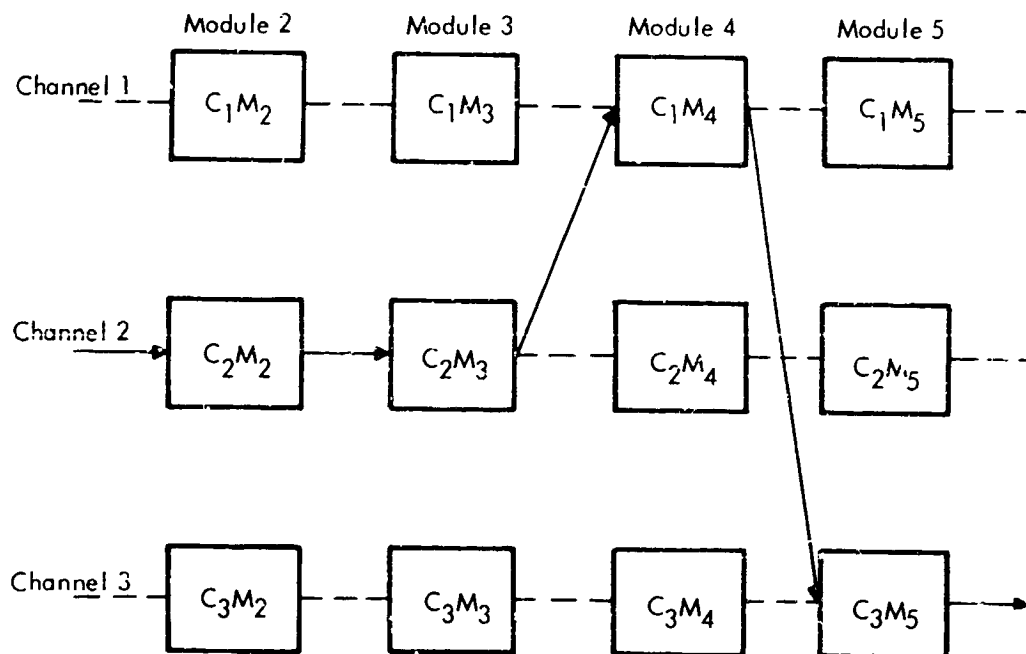


Figure 49. Module Switching

guidance and control computer, such studies would include an evaluation of the relative cost and merits of hardware and software methods of error detection and diagnosis. Since a basic ground rule was established for the AFS-EPO study that automatic methods and uninterrupted system operation were to be the primary criteria for trade-off, the hardware approach was followed wherever a choice between hardware and software existed. The resulting machine configuration therefore does not necessarily represent the optimum configuration for AES applications if uninterrupted system operation is not weighted as heavily as in the study and if component count is considered more important.

The hardware approach involved investigations of various methods of providing disagreement detection and of combining the disagreement signals in a manner to optimize failure isolation. Appreciable logic design effort was devoted to the problem of minimizing built-in test circuitry by combining the detection and voting functions in common logic. The feasibility of automatic switching to bypass failed elements was investigated with some success.

### 3.1.2 Software

As originally conceived, an appreciable study effort was to be applied to the design of test programs to support the logic simulation tasks and to the architecture (flow diagrams) of diagnostic programs to supplement the failure isolation capabilities of the hardware instrumentations. Existing Saturn-V test programs were found to be adequate for simulation purposes, however, and no new test programs were developed for this purpose.

Flow diagrams of programs capable of fault detection and isolation, sufficient to ensure proper operation of all channels of the computer and data adapter prior to any critical mission phase, were to be developed. However, since the hardware approach to failure detection and isolation was emphasized and since the hardware approach was extremely successful, little need remained for special diagnostic programming. This area of the study narrowed down accordingly to the definition of basic requirements for efficient detection and diagnostic programs based on simulation results.

### 3.1.3 Simulation

IBM developed a system simulator under the Saturn-V program to verify the logical integrity of the computer and data adapter, determine the effects of design changes, and evaluate test programs. Over a period of time, however, emphasis gradually shifted to special simulator applications where data concerning machine operation are generated to aid an operator in isolating detected errors. This simulator was adapted to the AES-EPO study to examine the error propagation effects of various types of component failures on the error detection and fault isolation capabilities of the AES computer and data adapter.

The Saturn-V system simulator is a set of IBM 7090 programs consisting of compiler, failure inspection, simulator, and diagnostic evaluation programs. The simulator flow diagram is shown in Figure 50.

The failure injection program allows cards containing selected failure identifications and descriptions to be read into the logic simulator on a failure injection tape. The failure injection program also produces a failure tape that the diagnostic evaluator program uses to compare actual injected failure data with the results of the simulator program.

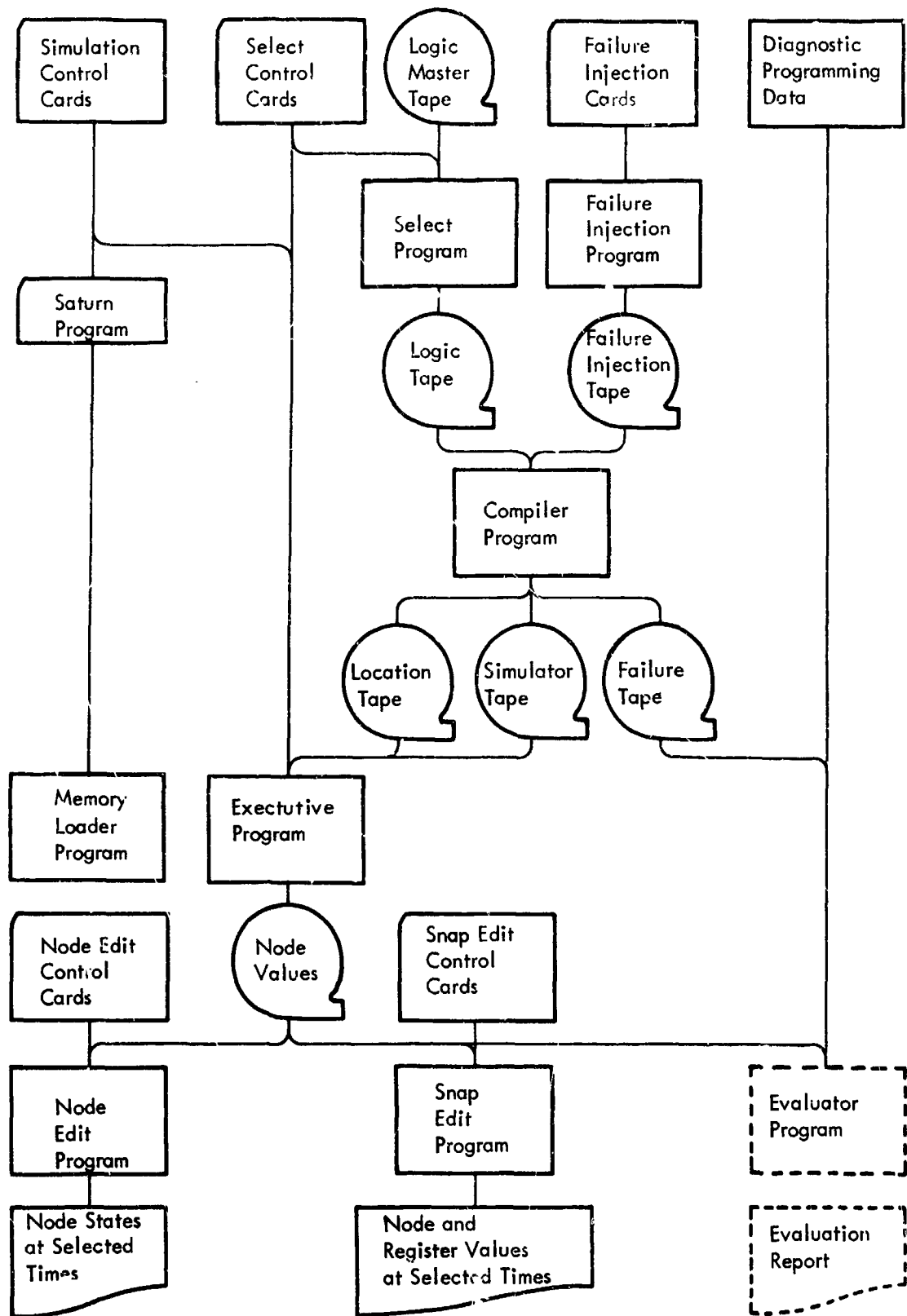


Figure 50. Saturn-V System Simulator Flow Diagram

The compiler program will produce 7090 instructions for the logic portion of the simulator program. The logic tape that feeds the compiler provides a detailed logical description of that portion of the machine selected from the logic master tape. The outputs of the compiler include (1) a simulation tape containing 7090 computer instructions for the simulator and (2) a location tape containing the assigned 7090 core storage locations for various logical element outputs.

The simulator program can determine system states while executing stored test or operational programs and can display on print-outs the state of selected nodes or register contents at any time during instruction execution. Simultaneous failure environments are provided by parallel simulation techniques; up to 25 multiple failures may be injected into each of 33 simultaneous environments. Up to 100 logical nodes may be monitored in either normal or failure simulation modes. Special pseudo operation codes allow additional selected nodes to be retrieved should the need arise.

### 3.2 Disagreement Detectors

In the TMR Saturn-V computer and data adapter, disagreement detectors provide an output if any of the triplicated modules fail. The disagreement detector consists of a three-way exclusive OR connected to each set of outputs of each trio of modules. There are approximately 200 disagreement detectors in the Saturn-V Guidance Computer. The outputs of several disagreement detectors are "OR'd" together to provide fewer outputs to the data adapter where an error-monitor register stores disagreement-detector outputs for telemetry transmission. The inputs to the disagreement detectors are clocked to allow time for the inputs to reach steady-state conditions before sampling.

Disagreement detector circuits can be made to sense errors between voter inputs, voter outputs, or channel input and voter output as shown in Figure 51. The Saturn-V instrumentation uses the method indicated in Figure 51a. Reliability requirements or module packaging configurations may dictate the need for using the method of Figure 51b. The method of Figure 51c is recommended for the AES configuration primarily because it indicates which channel is in error as well as which module.

Error detection and diagnosis studies were performed in the areas of optimum placement and timing of disagreement detectors in the AES computer and data adapter. Consideration was given to the problem of

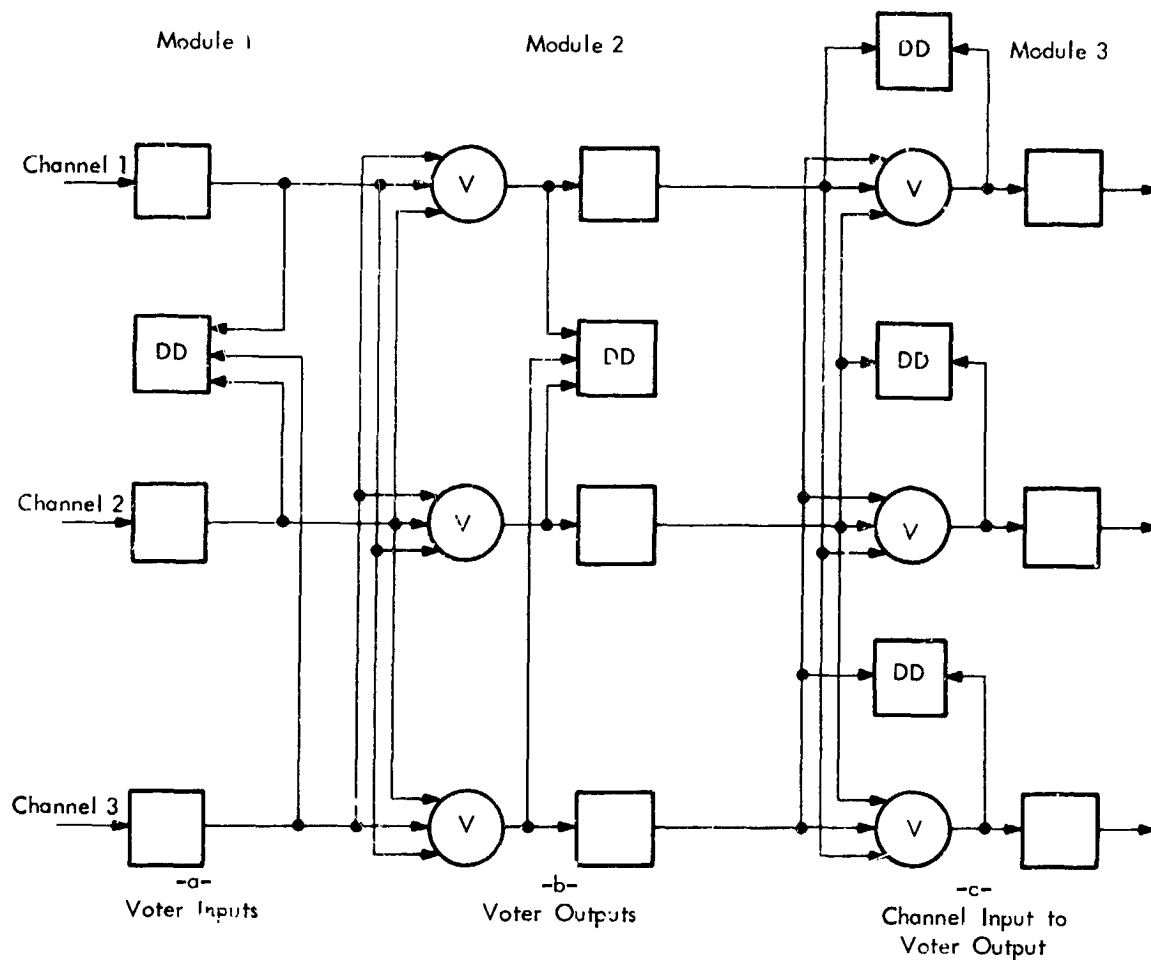


Figure 51. Methods of Error Detection

optimizing the "OR-ing" network for the detectors to provide failure isolation by means of disagreement signals to a replaceable module level.

Failure simulation experiments performed with the Saturn-V system simulator have shown that three error identification tags are required for failure isolation to a logic signal level using conventional

disagreement detectors as instrumented in the Saturn-V computer and data adapter:

- 1) Detection time of the error
- 2) Program instruction steps at times of detection
- 3) Error detector patterns.

Correct timing and placement of the disagreement detectors will provide the first two failure symptoms, and selective grouping of the disagreement detectors will provide the third.

### 3.2.1 Timing

The extensive propagation of errors through the computer presented the greatest problem in isolating failures to a replaceable module. Propagated errors tend to be sensed by many detectors, even though these detectors are not directly associated with the logic containing the failure, thus masking the source of error by "overdetection". An approach suggested during the course of the study of clocking the detectors only at the time that the associated logic is being used was found to require too much additional timing circuitry to be practical. Bit gates, phase gates, and in some cases even program step identification were found to be required to accomplish the desired detector timing. A method of combining the detector logic with the voter circuitry which would partially accomplish the object of optimum timing was investigated and is described in Section 3.3.

The Saturn-V disagreement detectors are clocked every like clock time (for example, any one disagreement detector may be clocked every x-time, another every y-time, etc.). As a result, detectors are sensing for disagreements between the simplex modules of TMR trios even at times when those modules are not being used by the program.

### 3.2.2 Placement

Error propagation has also been the major problem in attempting an optimum placement of disagreement detectors. Although failure isolation to a replaceable module level has been found to be feasible in the computer by reorganization on a functional basis and by redesign of the Saturn-V disagreement detectors, means must be found to prevent the error from propagating from one module to another and thereby destroying the isolation (as in the

case of timing signals). An approach was investigated in which each of the logic modules was partitioned into two or more diagnostic sections by placing additional detectors internal to the module to provide required isolation information.

The logic simulator was revised to allow flexible diagnostic partitioning and used to provide data optimum placement of disagreement detectors.

A logic simulation was designed to determine the optimum placement of disagreement detectors in the TMR logic. A total of 32 voters were failed and the failure data analyzed to determine the logic level to which the failures can be localized. The specific voters to be analyzed were chosen as representative of the various types of combinational and sequential circuits which would be "inputted" by the voted signals. The instruction and computer time when any of the module interface disagreement detectors sensed a failure was tabulated. An analysis of the simulation results showed that:

- 1) 53 percent of the voter failures could be identified by knowing which disagreement detectors had sensed the failed conditions.
- 2) 40.7 percent of the voter failures could be identified by knowing the program instruction and computer time of first detection in addition to which detectors had sensed the failed conditions
- 3) 6.3 percent could not be identified.

The partitioning of the reorganized computer resulted in using approximately 120 voters at the module interfaces. The simulation described assumed disagreement detectors at the input of each voter and nowhere else. The 6.3 percent of the voter failures which could not be identified was due to error propagation within a module and signal feedbacks between modules, resulting in identical error patterns for different failures.

This problem was alleviated by placement of additional disagreement detectors within the modules and at the module interfaces. To determine the number and location of the intramodule detectors, the four computer modules of the reorganized computer were divided into equivalent diagnosable subunits by physical count of the signal inputs to each of the latches and tratches in each of the modules. Table 28 summarizes the results of this count and indicates a measure of the unbalance of signals and voters (disagreement detectors) in each module.

TABLE 28 - Signals, Logic, and Voters

Module		Signal Inputs	Latches, Tratches	Voters (DD'S)
Number	Name			
1	Memory and Read	459	27	17
2	Arithmetic	1213	74	9
3	Control Timing	387	34	26
4	Operation and Decoder	720	69	45
	Timing (Distributed among four Modules)	135	13	23
Total		2914	217	120

Of particular interest is the ratio of the total number of signal inputs to the total number of voters (or disagreement detectors since the DD's were located at the voter inputs). This ratio was found to be 24:1. Using this figure as the basis for organization of equivalent diagnosable subunits, approximately 21 additional disagreement detectors were required. Their distribution and effect on the detector-to-signal ratio is shown in Table 29. The ratios are average values, which may be misleading because the additional detectors were chosen on the basis of individual circuit sizes within the module and on the basis of use and criticality. The effect of these additional 21 disagreement detectors was determined by simulation.

Based on component packaging density and intermodule wiring considerations, the AES computer was partitioned into four modules. Approximately 105 disagreement detector trios have been defined for intermodule failure detection. Table 30 shows the distribution of these detectors in the four modules.

The AES data adapter logic was partitioned into six modules containing a total of about 65 disagreement detector trios. In addition, 21 additional disagreement detectors monitor signals at the interface of the computer-data adapter unit.

**TABLE 29 - Additional Disagreement Detectors**

Module		Basic Ratio	Added DD's	Modified Ratio
Number	Name			
1	Memory and Read	27.0	1	25.5
2	Arithmetic	134.8	16	48.5
3	Control Timing	14.9	2	13.8
4	Operation and Decoding	16.0	2	15.3

**TABLE 30 - Distribution of Detectors**

Module	Function	DD's
1	Memory and Memory Interface	39
2	Arithmetic	9
3	Address Registers	27
4	Control	30

The partitioning of the computer into four modules and the data adapter into six modules seemed to be optimal from physical considerations such as the size of a replaceable module, the number of module interconnections, and the complexity of the computer-data adapter unit. Assuming that a disagreement detector is placed across each voter (comparing voter input and output signals) to isolate an error to the channel in a TMR module, and that a disagreement detector is also placed at the output of each voter trio to isolate voter failures from failures in the following logic as shown in Figure 51, then the partitioning described allows diagnostic error resolution by means of built-in circuitry alone (no special test routines) to a replaceable simplex level. Simulation results showed, however, that this was not an ideal diagnostic partitioning if the detector technique is restricted

to conventional Saturn-V disagreement detectors placed across voter inputs or if diagnostic resolution to a functional signal is required (because the generation of identical diagnostic symptoms from entirely different and unrelated signal failures resulted).

At present, no clearly defined ground rules exist which can be applied to optimally partition electronic units into diagnostic modules. Logic simulation has been used, instead, to determine the characteristics of failed machines and the nature of error propagation in a digital system to provide data from which such ground rules might be derived. Two simulation experiments were performed during the study to trace failure propagation through the computer logic. Sixty-six simulated failures were injected into representative voter interfaces and error propagation monitored by disagreement detectors placed at the input to every voter and at other selected logic nodes within the four modules of the AES computer. These nodes were selected on the basis of the total number of signal inputs to logic latches.

These experiments provided sufficient data to partition the computer into eight diagnostic modules although no change in the physical packaging of the four AES computer modules was considered. (The diagnostic module is defined by placement of disagreement detectors rather than by physical packaging.) The arithmetic module of the AES computer was partitioned further into three diagnostic modules, as was the control module. A comparison of error signal propagation between four and eight diagnostic modules is shown in Table 31 for sample failures. Note that there is less likelihood of identical failure symptoms occurring for failures in each of the four physical modules if the additional diagnostic partitioning is instrumented. For example, a failure in physical module 2 and another in physical module 3 caused identical failure symptoms in physical modules 2 and 3 when the computer was partitioned diagnostically into four modules but no identical failure symptoms when the computer was partitioned into eight diagnostic modules.

### 3.2.3 Detection and Resolution

The redundant mode was designed to be the operational and failure-detection mode of the Saturn-V computer. However, availability of a sufficient amount of failure data based on error-monitor indications allow a high degree of failure isolation. For this study, IBM simulated several hundred failures using the batch-simulation technique already described. Only single failures were injected into each simulated machine and each failed machine was exercised for the duration of the

TABLE 31 - Error Signal Propagation

Functional Partitioning

Interface Failure In Module	Symptoms Will Occur in Functional Modules			
Timing	1	2	3	4
1		2	3	4
2	1	2	3	
3	1	2	3	
4	1	2		4

Diagnostic Partitioning

Interface Failure In Module	Symptoms Will Occur in Dynamic Modules							
Timing	1	2	3	4	5	6	7	8
1				4	5	6		8
2		2	3	4	5	6	7	8
3		2	3	4	5		7	8
4		2		4	5			8

test program. As a result, a varying error-monitor pattern was generated for each failed machine.

Of the several hundred failures injected into the computer logic, less than 10 percent were undetected by the error monitors. These undetected failures involved either redundant logic elements or those included in the computer design to conserve power or insure against marginal conditions. A 99-percent failure-detection effectiveness was obtained after these types of failures were screened out.

The approach to failure isolation in the simulation was based on correlation of logic failures with error monitor patterns, pattern changes, and sequence of pattern changes. The simulation data indicated that about 75 percent of the failures could be isolated to a single logic module through examination of the error monitor patterns. About 90 percent could be isolated to one or two modules. In addition, examination of certain pattern characteristics - such as fixed-or-variable pattern, number of pattern changes during the test program, and sequence of error monitor changes - as the test program exercises various portions of the computer, logic provides an error resolution of one module for almost all of the simulated failures.

Table 32 is a portion of a typical print-out from the simulation of a redundant computer. The phase, bit, and clock time listed in the left-hand column is the instruction fetch time, but the simulator could be instructed to print out the actual time of occurrence of the error signal instead. The error monitor signals are represented by the 13 EP (error position) columns and the instruction sector and address location by the right-hand columns.

The simulator was instructed to print out a new line every time an EP location changed state. Consequently, only a small portion of the test program is listed in Table 32. The particular failures simulated in this run affected error monitor positions 12 and 19. Diagnostic information is contained not only in the generated EP signals but also in the instructions associated with a change of state of an error monitor and in the total number of changes in state, i.e., with the entire EP pattern.

Table 33 represents the results of another redundant simulation in which the simulated failures are associated with logic pages 1 and 2, and with error monitors 1, 2, and 3. An examination of the failure/monitor correlation alone (ignoring the additional diagnostic information given by the instructions and time sequences associated with state changes shown in Table 33). Table 33 indicates a high degree of

TABLE 32 -- Typical Print-out from Redundant Computer Simulation

INSTRUCTION FETCH TIME			ERROR MONITORS												INSTRUCTION	
P H A S E	B I T	C L O C K	E P	E P	E P	E P	E P	E P	E P	E P	E P	E P	E P	E P	S	A D R E S S
			0	0	0	0	1	1	1	1	1	1	1	2		
			1	2	3	4	1	2	3	4	5	6	8	9		
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	1	0	05 054
A	09	Z	0	0	0	0	0	1	0	0	0	0	0	1	0	05 057
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	1	0	05 060
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	0	0	05 062
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	1	0	13 037
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	0	0	13 042
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	1	0	13 043
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	0	0	13 051
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	1	0	13 054
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	0	0	13 061
A	09	Z	0	0	0	0	0	1	0	0	0	0	0	1	0	13 063
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	1	0	13 064
A	09	Z	0	0	0	0	0	1	0	0	0	0	0	1	0	13 226
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	1	0	13 227
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	0	0	13 232
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	1	0	13 233
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	0	0	10 212
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	1	0	10 213
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	0	0	10 222
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	1	0	10 223
A	09	Z	0	0	0	0	0	1	0	0	0	0	0	1	0	10 326
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	1	0	10 327
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	0	0	10 332
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	1	0	10 334
A	09	Z	0	0	0	0	0	1	0	0	0	0	0	1	0	10 341
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	0	0	10 342
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	1	0	10 344
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	0	0	02 103
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	1	0	02 104
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	0	0	02 111
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	1	0	02 113
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	0	0	02 201
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	1	0	02 202
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	0	0	02 203
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	1	0	02 204
A	09	Z	0	0	0	0	0	1	0	0	0	0	0	1	0	02 206
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	1	0	02 207
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	0	0	02 211
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	1	0	02 213
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	0	0	02 222
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	1	0	02 224
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	1	0	02 225
A	09	Z	0	0	0	0	0	0	0	0	0	0	0	0	0	03 012

TABLE 33 — Typical Redundant Computer Simulation

	EP 1	EP 2	EP 3
EP 1	Page 1 22%		
EP 2	Page 1 5%		
EP 3	Page 1 12%	Page 2 13%	Pages 1 and 2 25%

resolution between the two pages. Error monitor combinations EP1 alone, EP1/EP2, and EP1/EP3 were associated with failures injected onto page 1; error monitor combinations EP2 alone and EP1/EP3 were associated with failures on page 2; and error monitor EP3 alone indicated a failure on either page 1 or page 2. Failures thus isolated to page 1 represented 39 percent of the simulated failures, those isolated to page 2 represented 36 percent, and those which could not be resolved between page 1 or page 2 represented 25 percent. However, the 25 percent of unresolved failures could then be resolved by an examination of the full pattern equivalent to that illustrated in Table 33.

### 3.3 Switching

Module and channel switching, both automatic and manual, were considered in order to increase the reliability of the Saturn-V computer and the redundant version of the Apollo backup data adapter and to aid inflight maintenance. Single channel operation of some modules or of the entire computer-data adapter subsystem for noncritical mission phases was considered.

Two new modes of operation were considered for the AES computer system:

- 1) TMR/simplex
- 2) Switchable spare.

In the TMR/simplex mode, one or more modules of the system may be operated simplex while the remainder of the system operates TMR. One operational simplex module is turned off with every failed simplex module when that TMR module is switched to simplex operation. The switchable spare mode is an extension of the TMR/simplex mode in which the turned-off operational module is made available if a failure occurs in the operating simplex module. Switching problems associated with each of these modes were examined during the course of the study.

### 3.3.1 General

If the three signal channels can be made to function independently at the voter, simultaneous TMR/simplex operation is possible. The signal switching scheme is shown in Figure 52. Channel independency is obtained by forcing the voter input to a selected binary state regardless of the failed condition of the inputted logic. The failed logic module is switched out of operation along with a good module, and the selected simplex module operates with the other TMR modules. The key to TMR/simplex operational capability is in the method of using disagreement detectors to localize the failure to a module and switching voltages to control the flow of data through the voter circuits.

Voter designs using two different circuit technologies were studied for AES channel/module switching operations. The first (Saturn V) operates as a current summer feeding a threshold circuit. The second (integrated circuit - modified current switch) operates as a logic exclusive OR function ( $\text{vot} = A B + B C + A C$ ). Neither of these existing designs allow independent channel operation necessary for TMR/simplex mode capability, although both designs do allow simplex channel and simplex module operation.

Module/channel switching is accomplished at present by voltage-switch forcing of a binary one into one channel and a binary zero into another. In the Saturn-V instrumentation, a binary one is forced by grounding the +6 volt line to the logic AND gate preceding the voter, and a zero is forced by grounding the +12 volt input to the voter circuit. The present modified current switch instrumentation requires the outputs of preceding logic NOR gates to be forced. A binary one is forced by raising the reference supply of the NOR gate to the collector supply voltage, and a zero is forced by lowering the collector supply to the reference supply level.

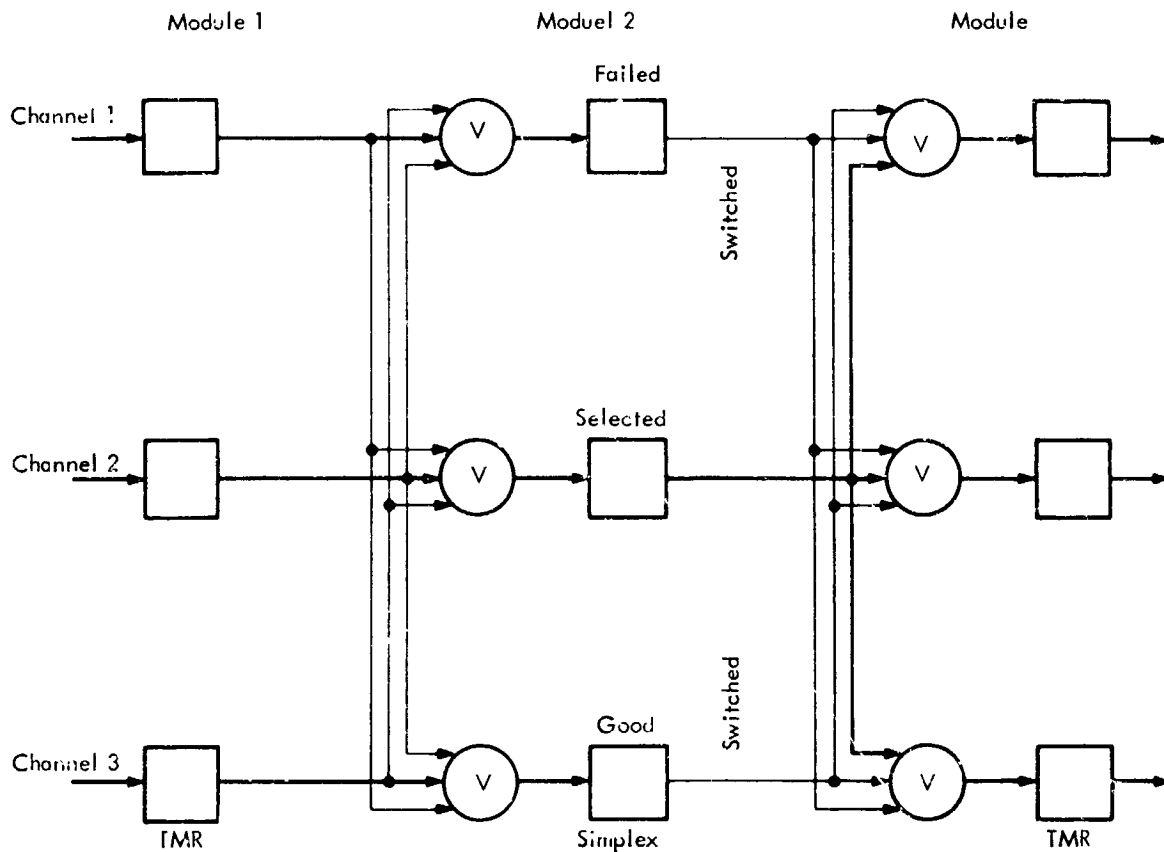


Figure 52. TMR/Simplex Operation

The desired TMR/simplex mode capability can be realized with the present integrated circuit design at the cost of additional logic and additional voltage planes. On the other hand, the Saturn-V instrumentation will require only a wiring modification consisting of: 1) supplying the voters with three independent +12 volt power lines which can be independently switched to ground level and 2) providing a switching capability on the -3 volt line which reduces the threshold level at the base of the voter transistor.

### 3.3.2 Switchable Voter

Considerable effort was devoted to investigating methods for using error correcting devices in lieu of the Saturn-V voters. Most of these methods permitted a switch down to one good channel in a trio

when another channel has failed. A constraint which was placed on the switching system was that control lines be kept to a minimum. For example, a control line for each individual error correction device was not considered to be feasible.

A switching device was designed with a capability of automatically switching from TMR operation on detection of an error in one channel to simplex operation of one of the two remaining channels. This automatic switch affects only the logic trio in which the failure occurred, all other trios remaining in the TMR mode. Propagation of errors is held to a minimum by using input error correction techniques rather than output error correction.

This design approach has two disadvantages compared to conventional majority voters. An intermittent failure causes switching to a simplex mode and does not recover its initial redundant state when the intermittent has ended, as does a voter circuit. Also, the switching device must have a preferred failure mode or else it will have a reliability no greater than the majority voter.

This first method was then extended to give an operator control over the switching. The logic trio would automatically switch to simplex operation upon occurrence of an error, but upon the occurrence of a second error, the operator could switch all trios involved in the module to the channel that has not failed. All other modules would remain in the TMR mode.

If the error was due to an intermittent failure, the operator could switch the module back to TMR mode when the period of the intermittent has passed. The disadvantage of this approach is that, to achieve an appreciable reliability gain over a voted system, the computer would have to be partitioned into a large number of modules. This would require a large number of error monitor indicators and switches, which the operator would be required to use.

To overcome the problem of differentiating between an intermittent and a solid failure, a third method was investigated in which the operator (or an automatic switching device) resets the switched-down trio and checks to see if the error is again detected. The first error encountered in each trio switches only that trio to one of the two remaining good channels. The two good channels are compared and if a second failure occurs to make them disagree, an automatic switching device on the trio output selects one of the two operating channels. There is a 50-percent probability that the automatic switch will select the remaining good channel. If it selects the wrong channel and the operator detects a system error, he can override the switch selection and select the remaining good channel.

Three disadvantages exist in this approach. The logic required to perform the switching function exceeds the other approaches. The method corrects only the first trio in any module having two channels that fail. Certain combination of failures will not alert the operator, and a diagnostic routine is necessary to enable the operator to detect a system error. However, since the system can continue to operate even when two channels of a trio have failed, the reliability of the system approaches that of a majority voting system with manual replacement of failed modules with spares. Also, each trio is switched independently of all other trios.

A fourth method was examined which was very similar to the third with the following exceptions. If the logic circuits have a preferred failure direction, the fourth method will have the same probability of selecting the proper channel as the failure preference. The AES computer subsystem contains a great deal of single-line transfer logic which does have a high probability of failure in one direction. However, the logic and interface required for the fourth method is greater than that for the third method.

Each of the methods examined provides specific advantages and contains certain disadvantages. Further study is required to select the best method for the AES computer subsystem.

The module/channel switching techniques considered for AES application were simple and straightforward but assumed the existence of a switchable voter design. The existing voter in the Saturn-V computer and data adapter is module or channel switched by forcing a logical one in one channel and a logical zero in a second channel. Since the "votes" of these switched voters cancel, the third channel effectively controls the voter output providing that no faults affecting voter operation exist in the equipment. Certain failures could exist in the Saturn-V design which might prevent forcing the two "switched" channels to the desired logical level.

Considerable effort was expended in reviewing technologies and developing concepts for switchable voting circuits. Although the primary requirement was a voter design in which the individual channel inputs could be forced to desired logic levels even in the presence of circuit failures, the capability to turn off individual channels was considered to be a more desirable feature. The "off" channels would be effectively removed from the circuitry and would present neither a logical zero nor a logical one to the voter.

The Saturn-V voter is a three-input current summing circuit in which the bias voltage sets the logical one threshold to two units of current out of three. This circuit could be converted to a switchable voter of the type desired by providing means of removing power at each of the channel inputs and simultaneously changing the bias so that the logical one threshold is set at one unit of current. Two channel inputs can then be turned off, and the voter operates as an inverter on the third channel.

An intuitively obvious approach to switchable voters was to consider logic voting as illustrated in Figure 53 rather than current summing as in the Saturn-V circuits. The output of the OR gate shown in Figure 53 is the AND signal of channels 1 and 2 or the AND of 2 and 3 or the AND of 3 and 1. If one channel (say 1) is in error, then the output of the OR gate is 2·3, the logic level existing on channels 2 and 3. Although the voting function is achieved, no practical means has yet been discovered to provide the desired switching function with logic circuits of this type.

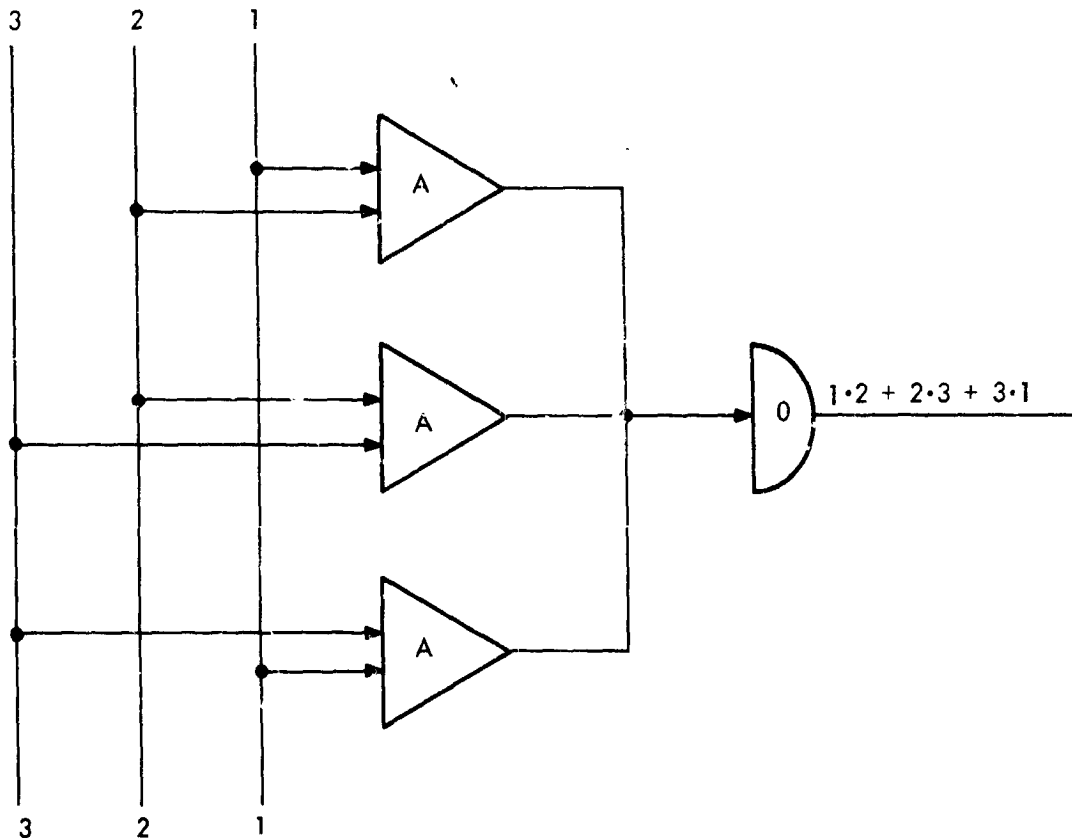


Figure 53. Logic Voter

### 3.4 Crew Requirements

A primary goal was defined early in the study to automate the error detection and fault isolation functions to the highest possible degree and thereby minimize crew requirements for inflight maintenance. Training, experience, and test information required by the crew to effect repair were made negligible by the hardware approaches pursued in the study. Man-in-the-loop operations required by the AES instrumentation were limited to reading a bank of indicator lights to determine the location of the failure and to making a manual replacement of the failed module. Semi-automatic repair methods in which the astronaut switches in wired-in spare units or changes mode were also investigated, as well as fully automatic repair and mode changing.

Test approaches and mechanical packaging approaches were directed towards eliminating the need for special test equipment or tools to effect inflight maintenance. No approaches were considered which could not be used by a suited astronaut.

### 3.5 Programming Requirements

The test programming requirements for AES applications were derived mainly from evaluation of existing Saturn-V programs and from simulation experience gained on this study and previous Saturn-V studies. Although the hardware approach to error detection and failure isolation taken in this study has minimized the need for special test programs, the following sections outline the program types and requirements for the general case where either a software approach might be emphasized or where a mix of the two approaches has been chosen.

The Saturn-V test programs consist of four primary types:

- 1) Memory load and verify
- 2) Computer self-test
- 3) Data adapter test
- 4) Marriage test.

The test programs required for the AES computer system would be similar except that the data adapter test and marriage test programs would be combined, since the data adapter is packaged with the computer in the AES configuration. Also, these programs would be useful

mainly for laboratory evaluation, since special test programs are not required for inflight error detection and fault isolation. The memory load and verify, or at least a simplified form of the one described in the following paragraphs would be used in flight.

### 3.5.1 Memory Test

The Saturn-V memory test programs are load and verify programs which exercise the memory circuits with selected instruction and data combinations. The programs are organized on a bootstrap principle in that operations progress from the simplest to the most complex tests. The programs are standard functional exercisers which force the computer to perform the following tests:

- 1) Checksum
- 2) One's Discrimination
- 3) Zero's Discrimination
- 4) Addressing
- 5) Checkerboard
- 6) Inverted Checkerboard.

The checksum test is a check of proper memory loading and operation of the test program.

The one's discrimination test checks the memories ability to write and read ones correctly. The memory buffer registers, sense amplifiers, core array, and driving circuits are checked by this test.

The zero's discrimination test checks the memories ability to write and read zeros correctly. The driving circuits are checked by this test, as well as the sense amplifiers sensitivity to noise.

The addressing test checks whether or not each memory location can be addressed correctly. The following circuits are checked in addition to the one's and zero's test: memory selection logic, diode matrix decoders, and all memory drivers.

The checkerboard and complement test produces maximum delta noise condition upon half read, which results in maximum inhibit noise whenever a zero is written. The inhibit noise from a cycle where zero was written can cause an error during the read portion of the next cycle.

The inflight memory load and verify program for the AES computer would probably be limited to address and checksum test routines, since the discrimination and checkerboard tests are for marginal conditions which tend to exist early in the computer's operational life ("infant mortality") or very late in life ("wearout"). These marginal tests would be a part of ground checkout before the start of the mission but would be of little value during the mission because the expected memory mission failures are catastrophic rather than marginal.

### 3.5.2 Computer

The Saturn-V computer test programs are functional exercisers which force the computer to perform each of the control, logic, and arithmetic operations for which the computer was designed. The programs are organized on a bootstrap principle in that the programmed operations progress from those which exercise the least amount of computer circuitry to those which exercise the most. In general, the order of test instructions is as follows:

- 1) Transfers
- 2) Shifts
- 3) One cycle arithmetic (ADD and SUB)
- 4) Logic (AND and XOR)
- 5) Multiple cycle, arithmetic (MPY, MPH, DIV)
- 6) Input/output operations
- 7) Interrupt

Within each class of instructions the test words also progress in a bootstrap manner. For example, a shift test would progress from shift high and low order bits to shift odd and even bits to shift all bits.

Although the computer test programs do not perform a diagnostic analysis of detected failures, they do provide diagnostic assistance to the operator by storing failure information.

Test data (literals) are used by the program in selected bit and word sequences to optimize test efficiency.

The test program is written such that the normal order of instruction upon detection of an error is to enter the error storage routine, store the error, and return to the main program at the next program step after that which detected the error. However, under operator control, the program may be halted to read available data, or the program may be recycled from the beginning.

The basic organization of the later Saturn-V test programs was changed from a bootstrap functional exerciser to a component-oriented, sandwiched-subroutine format.

The programs were generated by failing components systematically (on paper) and deriving subroutines to check each and every failure. The subroutines were then assembled in groups of 11 instructions followed by a special PIO, with given computer operations (such as multiply) distributed throughout the program. If this special PIO is not received at least every 11 instructions, the computer will assume a runaway or inactive condition of the test resulting from a malfunction. An alarm will be issued and the storage delay lines latched up. Instruction addresses were chosen to exercise all drive lines in all sectors during the program run.

The resultant test program provides advantages over a simple functional program, although the work effort involved in generating it is considerably greater. The component orientation of the program requires fewer instructions. The distribution of the computer functions throughout the program, rather than lumping each function in a particular portion of the program, provides a better inherent capability for detecting intermittents. Control of the test in the case of a computer malfunction which would normally disrupt the program is provided by the instruction grouping with the special PIO. Better diagnostic capability is provided through operator interpretation of the failure information and reference to logic analysis data which will be available.

An important conclusion from computer simulation is the apparent feasibility of constructing a diagnostic test program in which program branching is based on error monitor indications. The main program would be a short logic exerciser designed for efficient error detection only, and could operate periodically during the operational periods of the computer mission. If no error is detected, little operational time is consumed by the test. But if an error is detected, the program will branch to specific subroutines determined by the error monitor patterns.

In an actual development program, an "optimum" diagnostic configuration would be derived by a trade-off between hardware (built-in test circuitry) and software (test programs or routines). In the AES-EPO study, however, the hardware approach was selected whenever a choice existed, but consideration was given to the requirements for eventual diagnostic programs.

The majority of test programs are written by hand and are designed to test either every function or every component of the machine. The Saturn-V computer test programs were more than operation code exercisers. They were designed to bring to an up-level every diode line to an AND gate except the one being tested and to determine that the associated latch, latch, or inverter does not set or reset. Obviously, a complete and independent check of each diode cannot be achieved. Also, the bit pattern intended to test a specific diode will unintentionally test other diodes in other groups of circuits, and this situation will not be recognized when the program is being written. Only simulation will identify these multitest conditions.

Figure 54 shows the distribution of the disagreement detectors for a "minimum length" diagnostic program. Although this program contains 294 instruction program steps, the final failure propagation was determined by the 150th step. From these results, these observations were made: either the total program written to test out all the solid state devices was not needed or a better diagnostic symptom distribution could be had.

The diagnostic distribution can be increased provided the disagreement detectors can be properly timed. This is made possible by instrumenting the detectors to accept failures only at selective program steps. These steps are chosen to give predetermined failure symptoms. Control should be made available to operate the selected group of logic a set number of clock times.

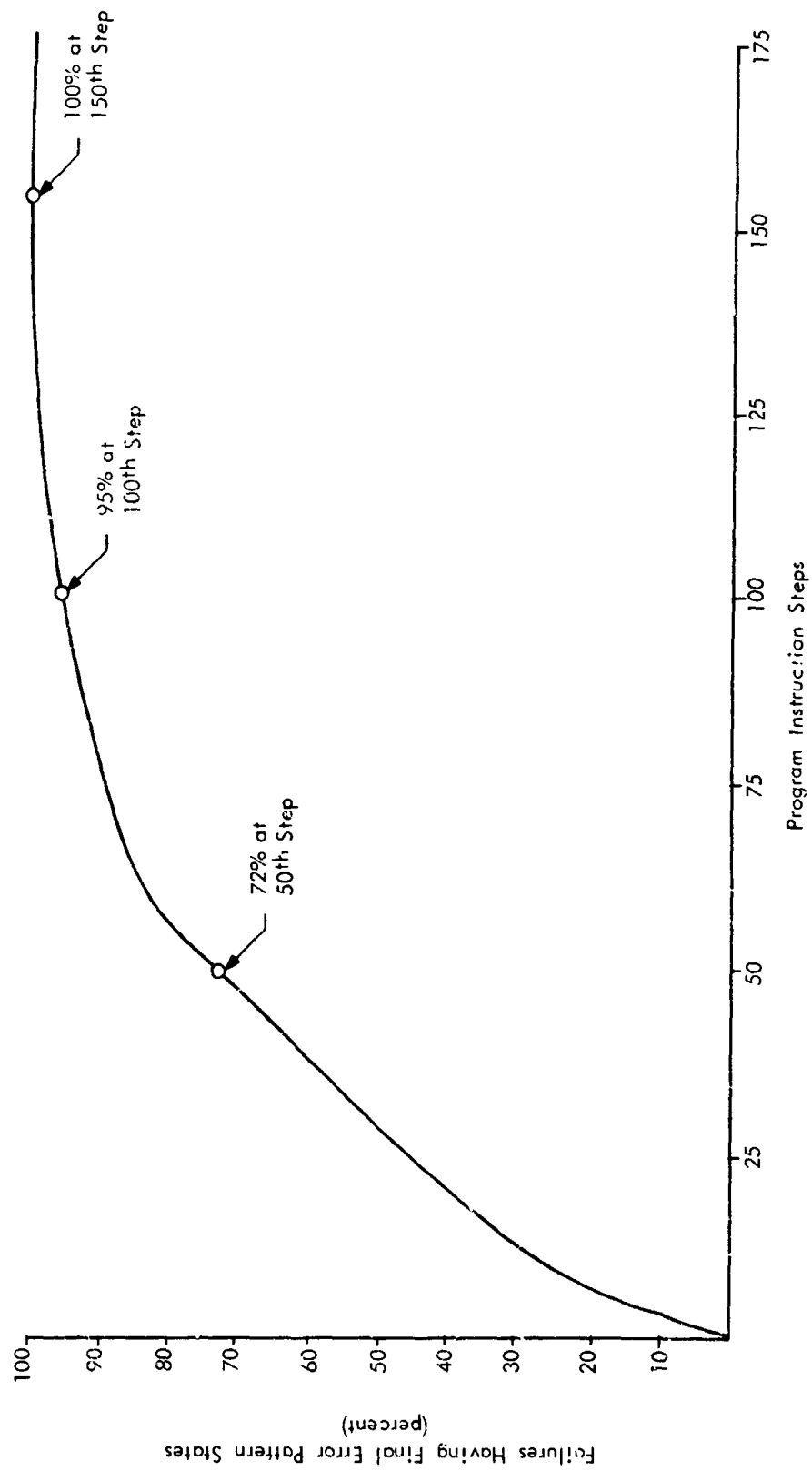


Figure 54. Detection Distribution in a Diagnostic Program

Many different types of symptoms were produced as a byproduct of the simulation experiments. All of these were analyzed to determine their individual and combined value in identifying logic signal failures. Table 34 gives a summary of these results. Signal failure identifications are based on the rearranged eight-diagnostic module configuration. Only unique signal identifications were tabulated.

TABLE 34 -- Symptom - Failure Correlation

No.	Observed Symptoms in Logic	Failures Identified (percent)
1	First Program Step of Detected Error	10.5
2	Final Error Pattern	26.3
3	Time of First Detected Failure	28.1
4	Final Error Pattern	20.2
5	First Three Program Steps of Detected Errors	63.2
6	First Three Program Steps of Detected Error and Final Error Pattern	96.5
7	First Program Step at Detected Error and Final Error Pattern	63.1
8	First Program Step of Detected Error, Final Error Pattern, and Phase, Bit, Clock Time of First Detected Error	82.4

To test the conclusions of the simulation experiments, a failure was physically injected in the computer by cutting a lead on an output of a logic inverter. The symptoms are given in Table 35.

TABLE 35 — Computer Symptoms

Instruction Step		Operation	Data Address	Error Position
Failure	006	CDS	121	-
	007	CLA	077	6
	010	MPY	100	6

The simulation problem was to fail all of the possible signals which could cause error position 6 to appear during instruction step 007. Based on the results of Table 34, approximately 63 percent of the failures could be uniquely identified if only the failure program step and final error pattern were given.

All the possible logic signals which could cause the error pattern were simulated to fail to the stuck "1" or stuck "0" case. As shown, only the HOP signal failure gave a duplicate symptom as observed in the laboratory. Indeed, this was the injected failure. Although failure isolation capability cannot be claimed from this single case, this is sufficient evidence that the simulation results are valid. A number of similar verified failure cases will have to be simulated to prove the worth of the diagnostic partitioning.

### 3.5.3 System

7 Saturn-V adapter test programs are similar in organization to the computer test programs being component-oriented rather than simple functional exercisers. The subroutines, assembled in functional groups of instructions, include the following tests:

- 1) Real time
- 2) Interrupts

- 3) Accelerometer processor
- 4) Ladder pulse counter
- 5) Discrete output register (DOR)
- 6) Switch selector register (SSR)
- 7) Buffer register
- 8) Mode
- 9) Ladders
- 10) Cross-over detectors (COD's)
- 11) Computer telemetry
- 12) Error monitor register
- 13) Discrete input multiplexer (DIM)
- 14) Data output multiplexer (DOM)

An error subroutine is forced upon program detection of an error, the normal order of instructions being to enter the error routine, store the error, and return to the main program at the next program step after that which detected the error. Error storage capabilities are provided for the first 46 errors occurring in the test run. Under program control, the program may be recycled through the subroutine in which the error was detected, the number of passes being predetermined by a constant. Upon completion of the subroutine recycling, the program resumes normal operation. Error data may be read out visually or by printout on operator request through the front panel switches.

The Saturn-V marriage test programs were designed to check out computer/data adapter combinations. Since the computers and data adapters used in the marriage tests were to have been checked individually before the marriage test, the primary purpose of these programs was to check the computer/data adapter interface and operational capability, especially in the area of timing.

In the AES configuration, since the computer and data adapter are packaged in the same unit, the data adapter and marriage tests would be combined into a single system test program. It is also possible to combine the computer and system test programs for the AES configuration except that there are advantages to applying functional test routines to the computer and operational test routines to the computer/data adapter system, which would be convenient to implement in two test programs rather than one.

#### 4.0 FABRICATION AND TEST

Limited fabrication was required in the study to prove the feasibility of inflight maintenance in a high humidity-zero gravity environment. Nine representative replaceable modules illustrating a solution to the problem of packaging and sparing in the adverse AES environment were fabricated by modifying Saturn-V Breadboard Computer No. 1 logic pages.

A nonfunctional mock-up of the AES computer subsystem was fabricated to illustrate the physical organization and packaging technique developed by the packaging and machine organization investigations of the study. A departure from conventional aerospace computer packaging illustrated by this mock-up is the elimination of over-all unit sealing in favor of individual module sealing.

Since over-all unit sealing was eliminated as a design feature, special consideration had to be given to the problem of providing adequate connector protection against long-term exposure to the high humidity-zero gravity AES environment. Exploratory tests of various connector sealing methods resulted in a gasket-silicone gel technique which showed no appreciable change in leakage resistance between contact pins even when unmated and remated in a salt water bath.

Fabrication of a special environmental test chamber was necessary to provide a simulated AES environment for evaluating the representative modules. This chamber provided a controllable humidity, a periodic spray of a solution of sodium chloride and urea in water, a controllable duty cycle on the test modules, and a means for disconnecting and reconnecting the modules in the environment to simulate maintenance operations.

Evaluation tests were performed on the nine representative modules in the special test chamber. These tests were exploratory rather than demonstrative in nature. The environmental stresses such as humidity, temperature, contaminants, and disconnections were gradually increased over a test period of several weeks in order to determine by what margin the modules meet the operational requirements rather than simply whether they qualify or not.

##### 4.1 Computer Mock-Up

A nonfunctional mock-up of the AES computer system was fabricated to illustrate the organization and packaging concepts developed

during the study. A general layout of the mock-up is shown in Figure 55. The computer and data adapter are packaged in the same structure although there may be some installation advantages to packaging them separately as in the Saturn-V system.

The recommended structure would be made of magnesium-lithium and is designed for integral cooling. Since the AES computer will not be a sealed unit as in conventional aerospace designs, no provision for over-pressurization, relief valves, or purging were required. Most of the electronic components are packaged in thirty logic modules, three memory modules, and four power supply modules (including an RFI filter). Twelve additional logic modules are included as spares or growth potential. A large screw located in each module provides a positive connect-disconnect technique for the logic pages and eliminates the need for special tools such as the Saturn-V page puller. Each module is individually sealed. The structure itself is hermetically sealed and contains the interconnection boards and cables for the modules.

A photograph of the completed mock-up is shown in Figure 56 in the Appendix.

#### 4.2 Exploratory Tests

Whatever packaging technologies are eventually selected for AES applications, the problem of sealing the intermodule and interequipment connectors against the high humidity-zero gravity environment will exist. Exploratory testing of methods of sealing the Saturn-V page connectors resulted in the selection of a gasket-silicone gel technique for the representative module to be demonstrated according to the Phase II test plan. A sketch of the representative module is shown in Figure 57.

A request to use Saturn Computer Breadboard No. 1 logic pages in the AES-EPO study to test various methods of protecting against the high humidity-zero gravity environment was approved by NASA-MSFC. These breadboard pages were modified by sealing the pages with a potting compound (RTV). Since thin laminar coatings (as used on Gemini and Saturn-V pages) were found to be porous and since thick encapsulant coatings were found to damage connections and components during curing, a technique was developed for the AES modules in which a thin laminar coating was applied to the page surfaces to protect the circuits mechanically from the thick layer of encapsulant which was then applied over the laminar to provide a nonporous seal. The modules

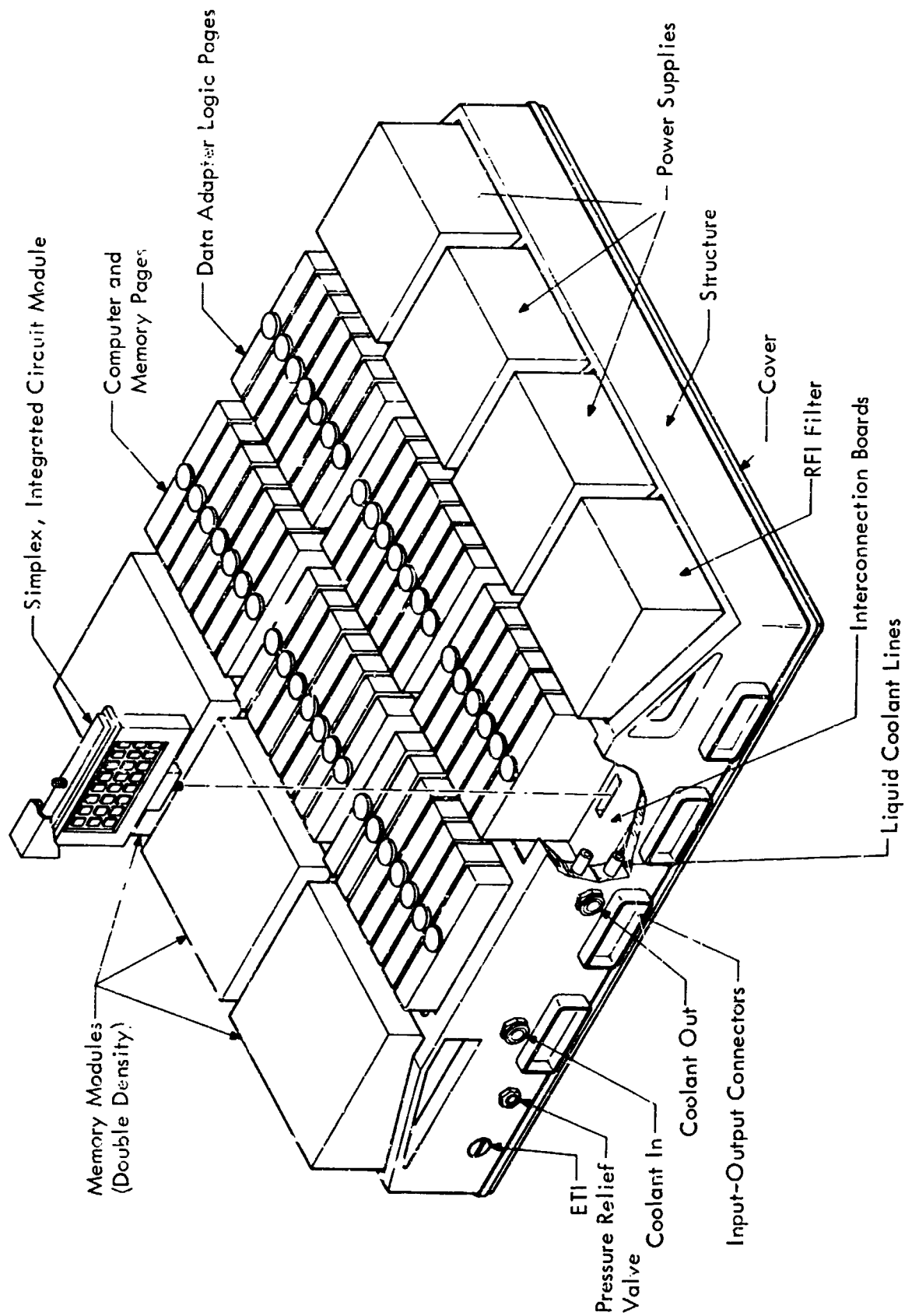


Figure 55. Apollo Computer - AES

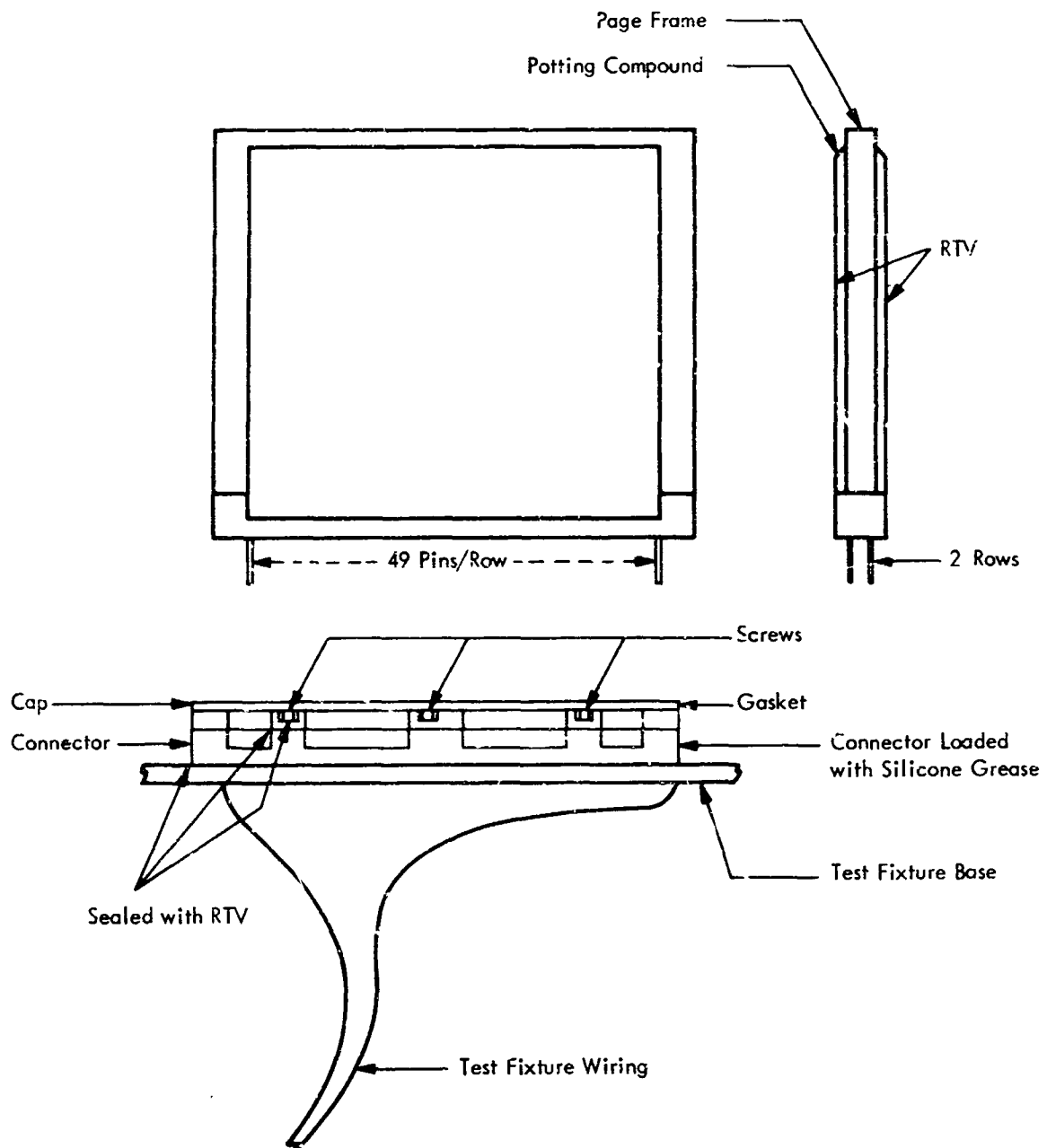


Figure 57. Representative Module for Phase II Testing

were baked and evacuated before treatment to avoid sealing in moisture. The female connector, wired into the test fixture, was sealed with a silicone rubber gasket on top with an RTV seal around the sides and was loaded with silicone grease to retard moisture accumulation in the female pins.

Phase I testing included the following investigations:

- 1) Gasket seals on the interface between the male and female connectors
- 2) Sealing of the connector with various greases
- 3) Combinations of the above.

The technique showing the most promise is sketched in Figure 58. Male and female Saturn-V page connectors were wired and sealed with epoxy on their rear surfaces. A silicone rubber gasket was glued to the face of the female connector with Dow-Corning A9-4000. The female cap was removed and DC-3 silicone grease packed inside the connector. The pins of the male connector were also saturated with DC-3 silicone grease. Contact measurements before and after application of silicone grease indicated that the grease had no measureable effects on the contact resistance between male and female connections. Leakage resistance checks between adjacent pins showed the following worst-case conditions:

- 1) Initial leakage resistance of mated test model--500,000 megohms
- 2) Immersed mated connector in fresh water for 15 seconds and shook off excess water--2,000 to 10,000 megohms, erratic
- 3) Unmated connector, dried male for 20 seconds at 125 degrees Fahrenheit, remated--140,000 megohms
- 4) Unmated connector, immersed both halves in fresh water for 15 seconds, shook off excess water, remated--70,000 megohms
- 5) Unmated connector and remated--5,000 megohms
- 6) Unmated connector and remated--70,000 megohms

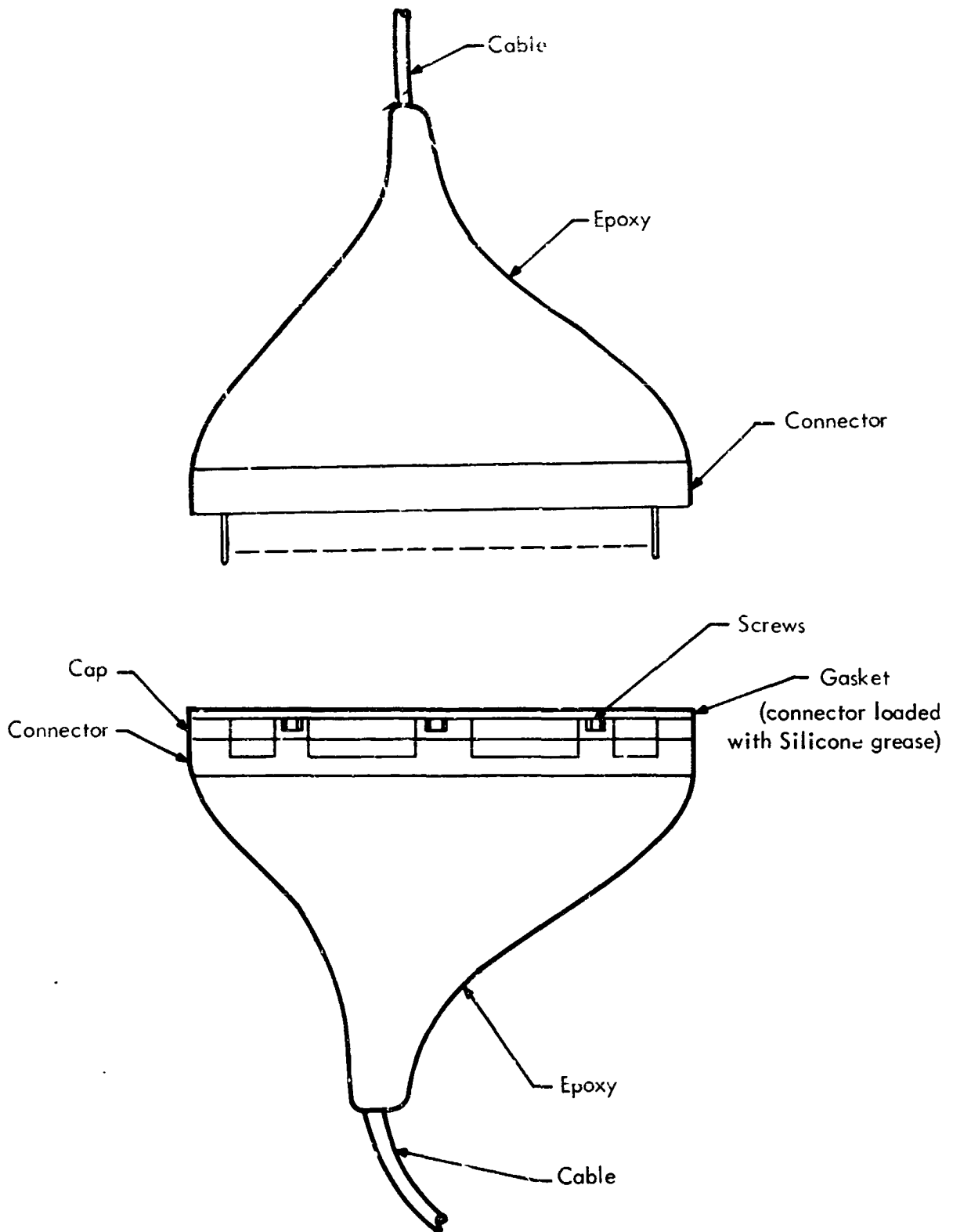


Figure 58. Phase I Test Model

- 7) Unmated connector and remated--85,000 megohms
- 8) Unmated connector and remated--60,000 megohms
- 9) Unmated and remated connector under fresh water--reading erratic
- 10) Unmated connector and shocked water off male on desk top, remated--50,000 megohms
- 11) Unmated connector and remated--10,000 megohms.

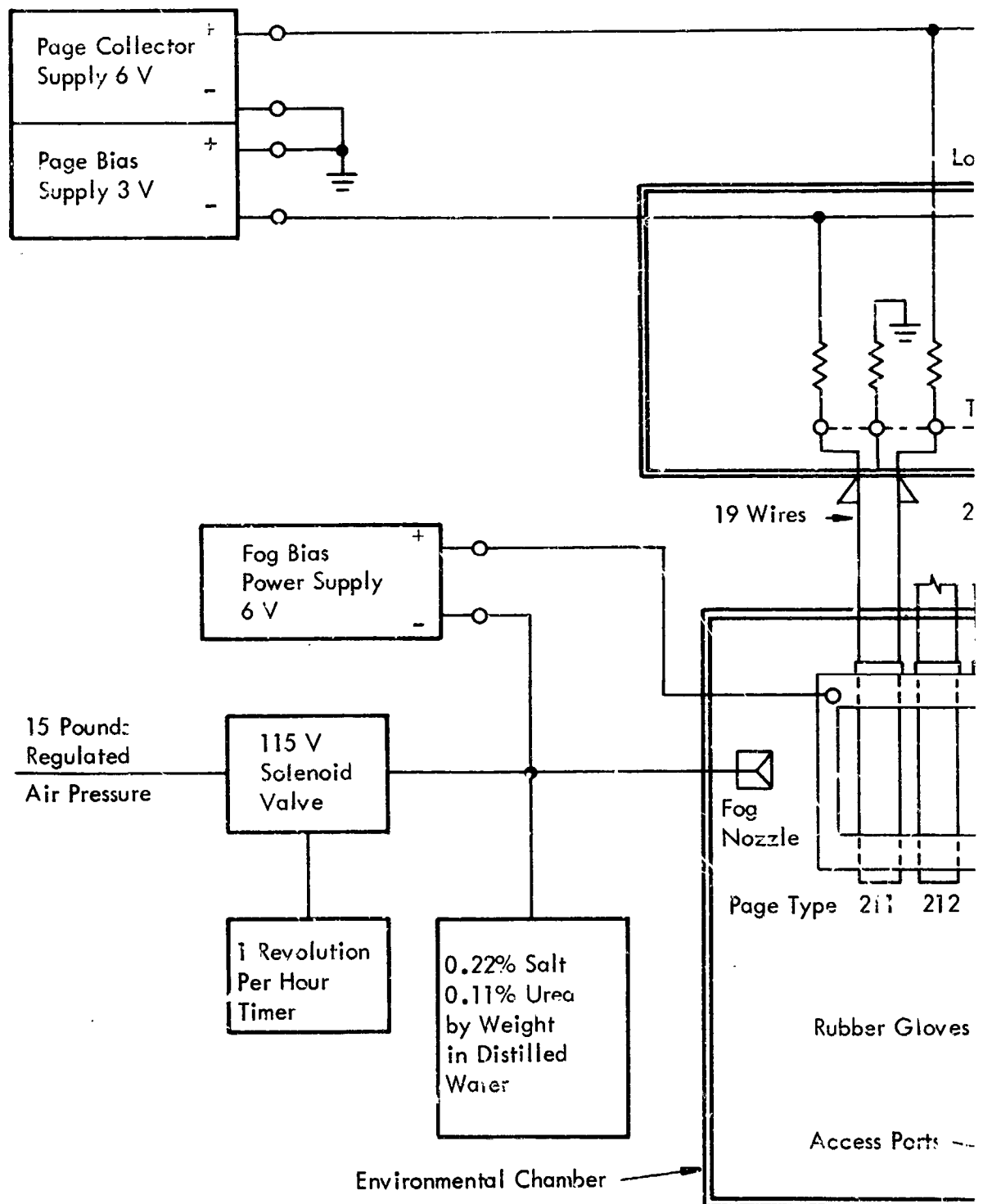
Previous tests of a similar nature with gaskets alone and with greases alone resulted in low leakage resistance readings. Although the readings listed above appear erratic, they were very encouraging from the following viewpoints:

- 1) The lowest leakage resistances were still in the thousands of megohms.
- 2) The surface between the cap and connector of the female, and the screw holes in the female, presented sources for leakage which were sealed during Phase II tests.
- 3) Additional exploratory testing with a lighter silicone grease did not exhibit as erratic readings as above even though the water bath was changed to salt water.

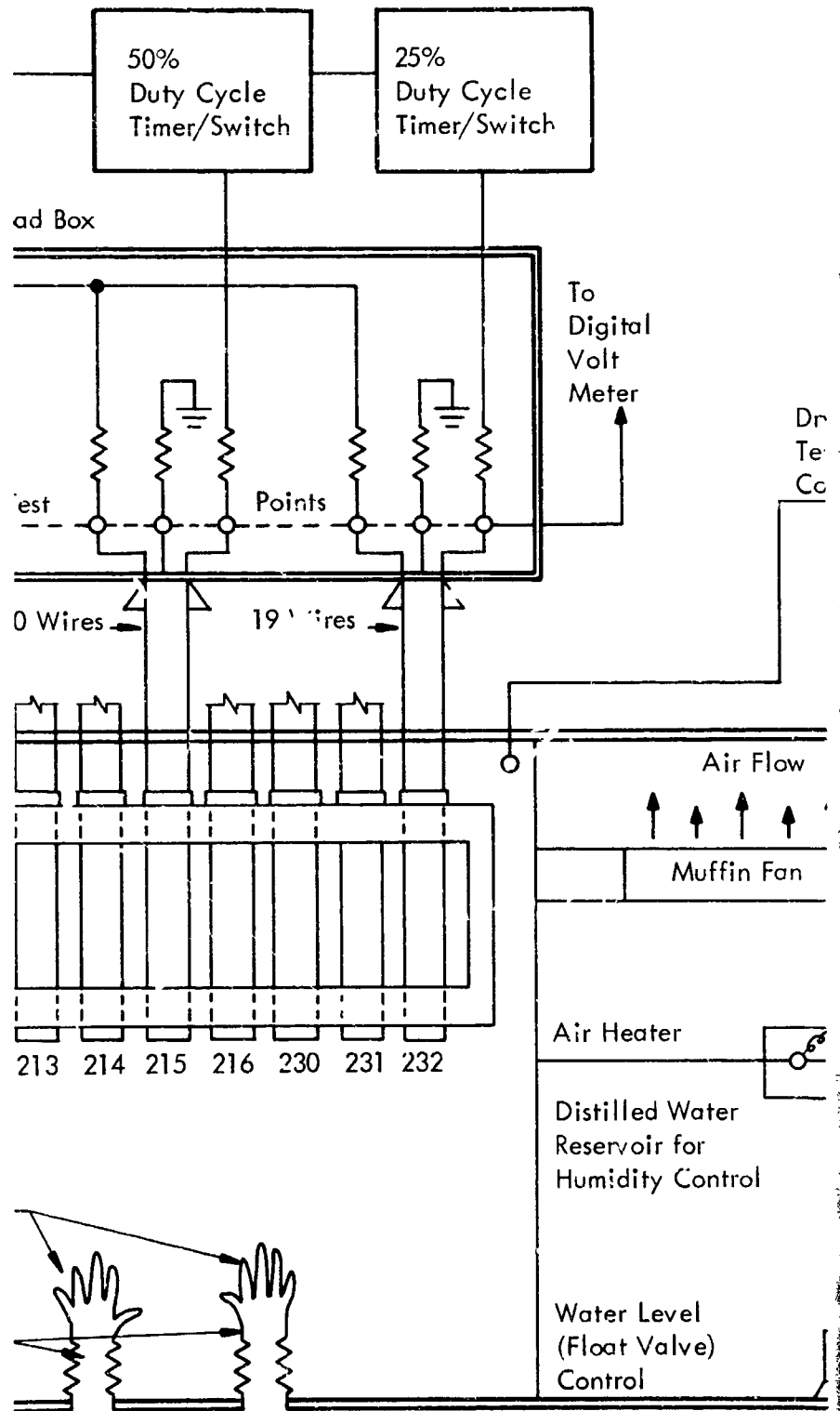
#### 4.3 Environmental Simulation Equipment

A special environmental test chamber was required to simulate the high humidity-zero gravity AES environment. A photograph of the chamber is shown in Figure 59 in the Appendix, and a functional diagram is shown in Figure 60. Test equipment used in Phase II testing is shown in Table 36. The chamber was designed to provide the following nominal environmental conditions with means for varying these conditions over a wide range:

- 1) Relative humidity of 90 percent
- 2) Temperature of 100° F



1130



173②

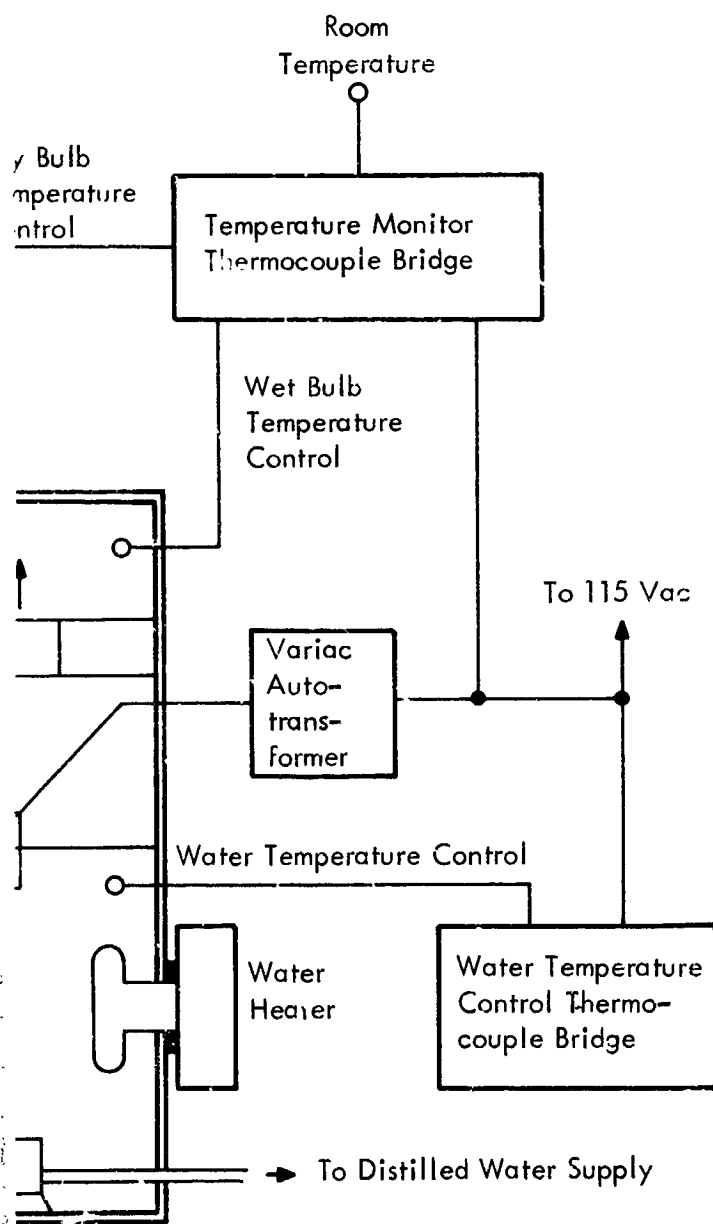


Figure 60. Functional Diagram - Test Chamber

TABLE 36 — Test Equipment Listing

Unit	Type
Page collector power supply, +6v . . . . .	Trygon Mod. S36-2.5
Page bias power supply, -3v and 6v fog charge power supply. . . . .	Twin low voltage by Harrison Labs. Mod. 802-B
Duty cycle timer switches . . . . .	Paragon Model 4001-0
Solenoid valve, 115 Vac. . . . .	
Timer - one revolution per hour - for fog spray . . . . .	Haydon
Muffin fan for air circulation . . . . .	Rotron Corp.
Digital voltmeter . . . . .	Kintel Mod. 456
Digital readout . . . . .	Kintel Mod. 473-A
Water temperature controller. . . . .	Honeywell; Mod. 152C33P-36-11
Water level control . . . . .	Water Boy by Maid-O-Mist Co.
Water heater . . . . .	Chromalox-220v- 2000 watt, Edwin L. Wiegand; Pittsburgh, Pa.
Air heater. . . . .	100v 'Hot Watt' - car- tridge type with 10 1-1/2" square of 0.08" copper soldered to heater
Air heater control . . . . .	Variac. - General Radio - Type W10MT3
Temperature control bridge readout . . . . .	Honeywell Mod. 15618826-06-01-2-061

- 3) Water with 0.22-percent sodium chloride and 0.11-percent urea in solution sprayed on test modules once each hour to simulate the attraction of free water to an electrical field under zero gravity conditions
- 4) Electrical charge applied to spray prior to contacting modules to simulate ionization of free water
- 5) Duty cycles imposed on modules of 25, 50 and 100 percent.
- 6) A source of hot air for drying the module connector after it has been removed from its receptacle, sprayed, and before it is reconnected to simulate a possible maintenance technique (not used during entire test)
- 7) Rubber gloves sealed to one wall of the chamber to allow simulated maintenance activity (module replacement) without changing the environmental conditions (and possibly simulating the suited astronaut conditions).

A photograph of the chamber in operation is shown in Figure 61 in the Appendix.

The following Saturn V Simplex Breadboard No. 1 pages (replaceable modules) were placed on test after potting modifications:

1)	Transfer Register 1	6109211
2)	Multiply and Divide 1	6109212
3)	Operation Code	6109213
4)	Transfer Register 2	6109214
5)	Interrupt	6109215
6)	Sector Register Y Decode	6109216
7)	Multiply/Divide 3	6109230
8)	Arithmetic Instruction Counter	6109231
9)	Address Register and X Decode	6109232

Twenty functional connections were chosen for each logic page, and d-c voltages were applied to the input terminals of this connection set. The d-c patterns at the output terminals of each logic page were then monitored periodically during the test period to determine if the environment had caused a deterioration of the logic pages or connectors.

Photographs of the test fixture containing the nine representative test modules are shown in Figure 62 in the Appendix.

#### 4.4 Evaluation Tests

The fabrication tasks required by the statement of work were directed at solving the long term reliability problem by sparing. However, inflight maintenance in a zero gravity is complicated by the fact that free water in the form of droplets, migrating to points of electrical potential difference, exist in the spacecraft environment. Consequently, it was necessary to solve the problem of sparing in this environment before inflight maintenance could be utilized as a means of meeting high reliability apportionments for long term missions.

Nine functional computer modules (Saturn V breadboard pages) were packaged using the technique determined by exploratory testing to be the most suitable for successful operation and maintenance in the AES environment. All test modules and their mating receptacles were visually examined to determine and record their condition prior to test. Each module was initially checked electrically using the following procedure:

- 1) Module placed in the receptacle.
- 2) Resistance measurements made from its external load resistors to either ground or the +6 volt power supply.
- 3) Power applied.
- 4) Current flow through each of the 20 activated pins was determined by measuring the voltage drop across the load resistors. (Voltage sources have 10-ohm resistors in series with their pins.)
- 5) Power was turned off and the module removed.

All modules were placed in their receptacles, power applied, and currents checked. Voltage planes were supplied. Their nominal voltages and logic inputs were supplied with d-c levels.

Environmental conditions described in Section 4.3 were applied and the test initiated.

Functional operation of the modules was checked daily for the first five days of testing and twice a week thereafter.

Duty cycle total number of removals and replacements, and number of times each module was sprayed while disconnected from its mating connector are indicated in Table 37.

TABLE 37. Test Schedule

Module Number	1	2	3	4	5	6	7	8	9
Duty Cycle (%)	100	100	100	50	50	50	25	25	25
Removals/Replacements	0	0	2	0	0	2	0	0	2
Sprays while removed	1	1	2	1	1	2	0	2	2

Plus 6-volt power was turned on and off once each 24-hour period to achieve duty cycles less than 100 percent.

Removal and replacement of the modules was performed manually by utilizing rubber gloves fitted to the wall of the chamber. Modules were removed from the mating connector for approximately 3 minutes to simulate a maintenance action.

For each replaceable representative module, a log was maintained containing a detailed time history of modification and test events, including all pertinent environmental and test data. These logs remained with their respective modules throughout the study period.

#### 4.5 Test Results

Phase I (exploratory) testing of various methods of sealing module connectors resulted in the selection of a gasket-silicone gel

technique. Although the purpose of Phase II testing was to evaluate this method of sealing the module connectors in a simulated high humidity - zero gravity environment, the Saturn-V logic pages used the represent AES replaceable modules had to be sealed as well to prevent logic failures during test. Unfortunately, the magnesium frames of the logic pages deteriorated during the course of the test, allowing moisture to work between the decomposed frames and the RTV sealing compound, and logic failures did occur. However, since the purpose of Phase II testing was not to evaluate sealing of the module itself (replaceable modules in the AES computer would be hermetically sealed as individual components) and since only one connector failure (a loose gasket) could be identified during the entire test period, the gasket-silicone gel sealing technique for electrical connectors was felt to be demonstrated as a feasible solution to connector operation in the adverse AES environment.

Very few test points on the nine representative modules showed any appreciable change in voltage level during the first month of testing although the magnesium - lithium frames of the Saturn-V logic pages showed drastic deterioration. Those test points which did exhibit appreciable change (over 5 or 10 millivolts) were found to be located on those pages showing the most frame deterioration, indicating that the voltage changes resulted from moisture leakage around the frames (under the RTV seal) rather than at the connector.

On 7 November the tests were interrupted by a failure of the test chamber. A connection came loose from the water tank causing a flooding condition and drastic changes in the temperature - humidity environment. A rash of voltage changes occurred at this time, especially on those modules exhibiting the most frame deterioration.

#### 4.5.1 Electrical Measurements

It is difficult to define a voltage change as a failure, since the operation of digital systems is on-off in nature. Even the most drastic changes in voltage levels monitored during the test may not cause a logic failure in actual practice. For the purpose of this discussion, however, a logic failure is defined as a voltage change of over 25 millivolts.

Of the nine representative modules, six exhibited no failures until the test chamber failed (a test period of over a month). Two modules survived the flood and exhibited no failures for the entire test period (57 days). One module exhibited one failure, and a second module

exhibited two failures after the flood. One of the modules which operated perfectly up to the time of the flood had to be disconnected following the test equipment failure because it began to draw excessive current from the power supplies.

One module exhibited two failures during the first month of testing. Another module lasted 20 days of testing before experiencing its first failure and then degraded rapidly. The ninth module experienced three failures after only a few days of test and then stabilized until the flood, after which it degraded steadily.

Only one module out of the nine had to be removed from the tester due to drawing excessive current, however. Eight finished the test period of 57 days.

In general, the frequency of failures could be correlated with deterioration of the magnesium-lithium frame (causing the RTV seal to peel off the circuit board). The failure mechanisms seemed, therefore, to be moisture leakage under the edge of the RTV seal rather than by means of the connectors. Detailed examination and dissecting of the failed modules supported this conclusion.

The failures (defined as a change in voltage level at the test points of greater than 25 millivolts) are charted for each of the test modules in Figures 63 through 71. A number of recoveries (return of test point readings to within 25 millivolts of the original reading) were identified during the tests and denoted by downward pointing arrows on the charts. The chamber failure occurred at 936 hours.

As an example of how to read the charts, refer to Figure 63. No failures occurred until the chamber flooded. The voltage level at seven test points shifted by more than 25 millivolts at this time. Another failure occurred at about 1125 hours but recovered 2 days later. The test point levels then remained unchanged for the remainder of the test.

The total failures of all nine modules are plotted in Figure 72 as percentage of test points failed versus test days. This plot is of some interest since a continuous curve drawn through the discrete test data points generally follows a typical logistic curve (growth modified by a limiting factor). If this figure does represent a logistic trend, it indicates that additional failures would occur at a slower rate if the test period were extended for an additional period of time. The "growth" (exponentially increasing) portion of the curve could be due primarily to deterioration of the magnesium-lithium frame, and the "constraint" (leveling off of the curve) could be due to the better protection afforded

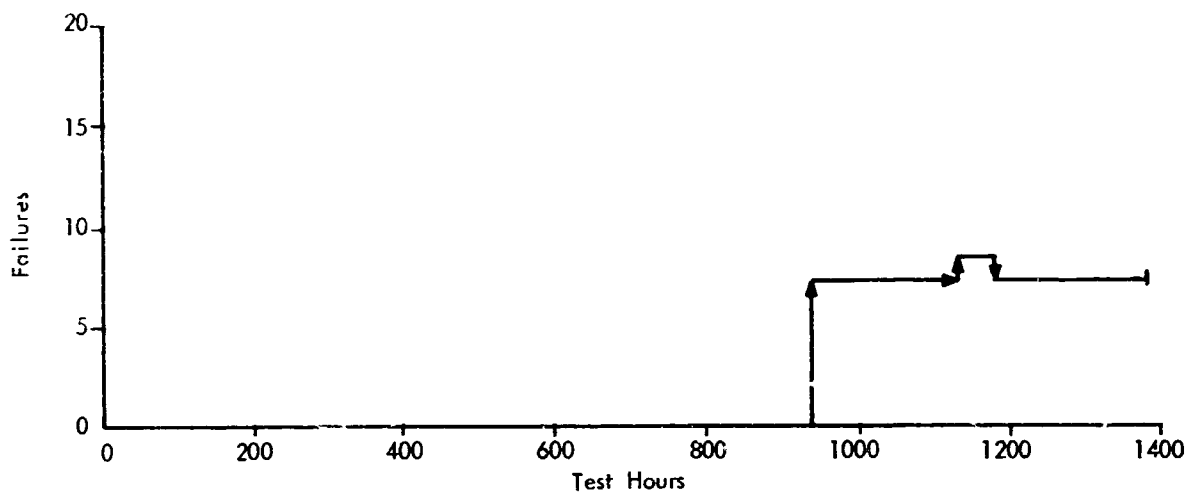


Figure 63. Phase II Module Failures (>25 Millivolts) - Module No. 211

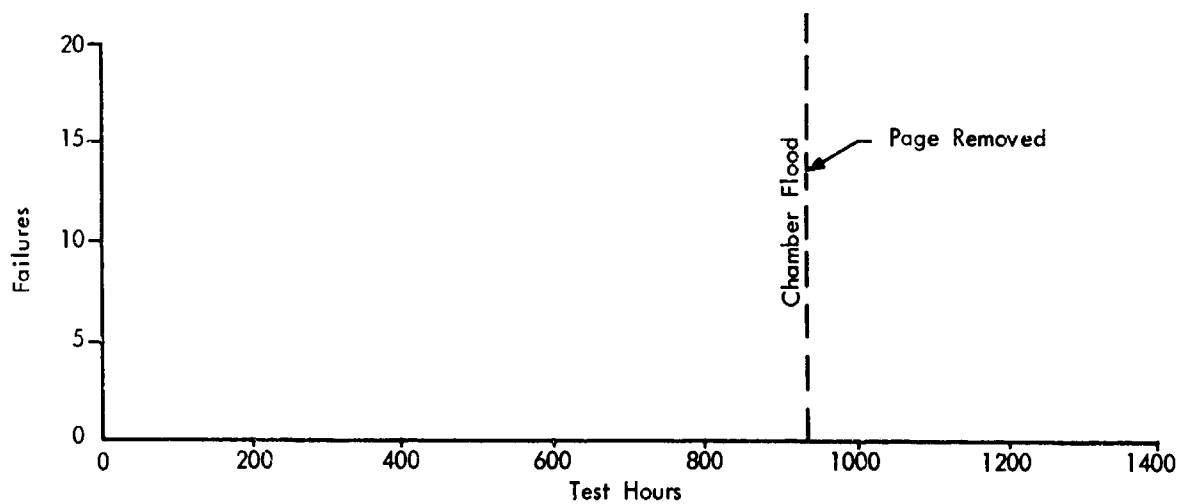


Figure 64. Phase II Module Failures (>25 Millivolts) - Module No. 212

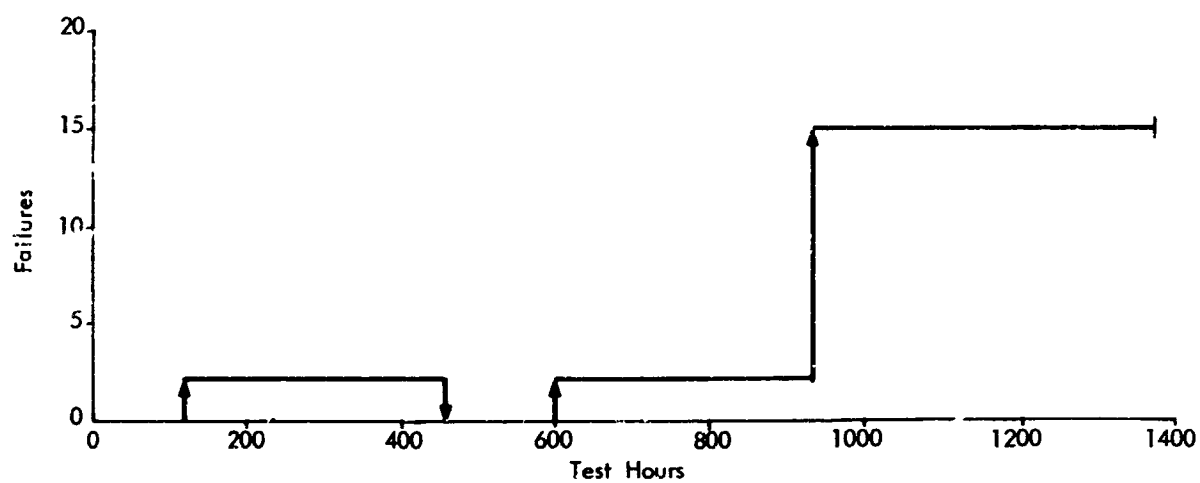


Figure 65. Phase II Module Failures (> 25 Millivolts) - Module No. 213

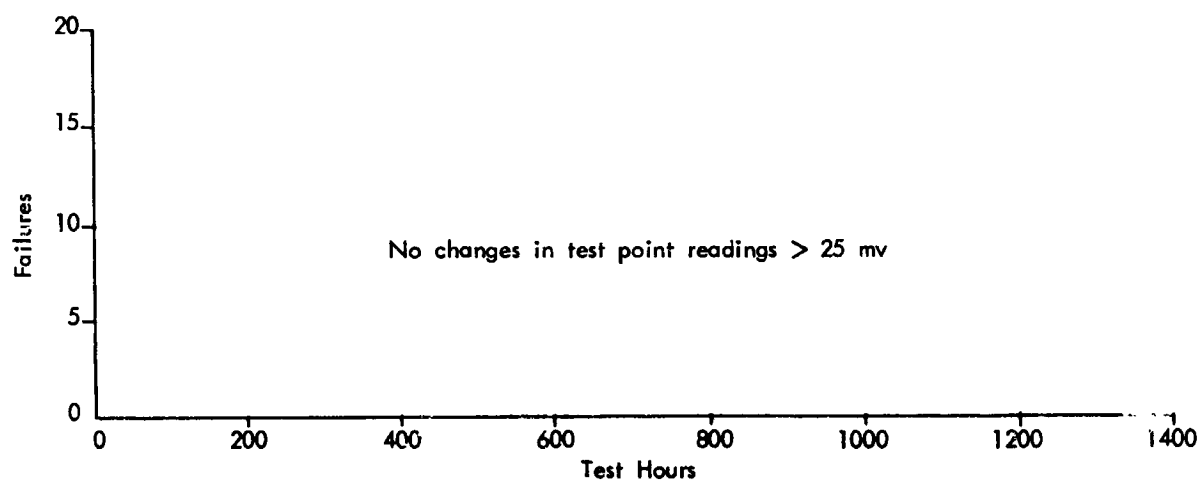


Figure 66. Phase II Module Failures (> 25 Millivolts) - Module No. 214

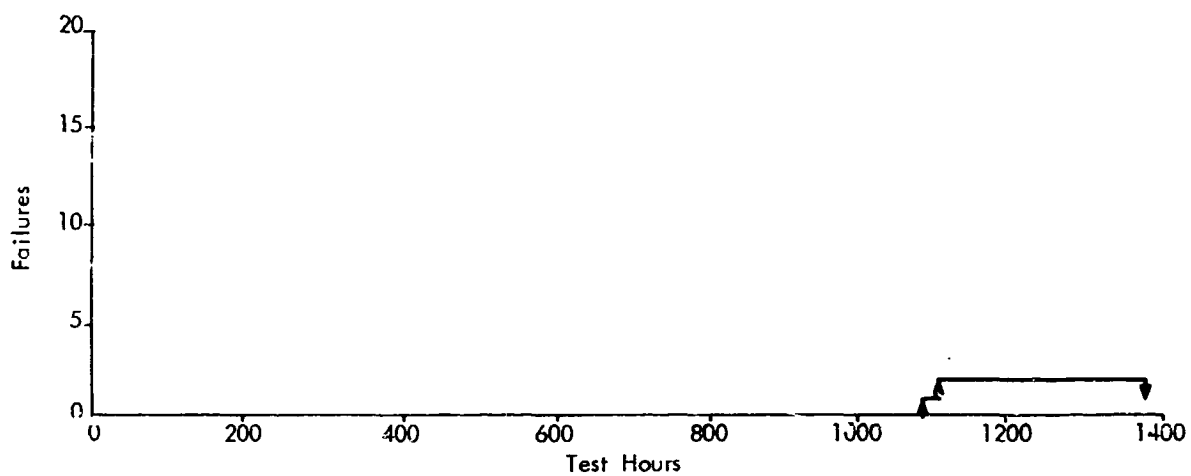


Figure 67. Phase II Module Failures ( >25 Millivolts) - Module No. 215

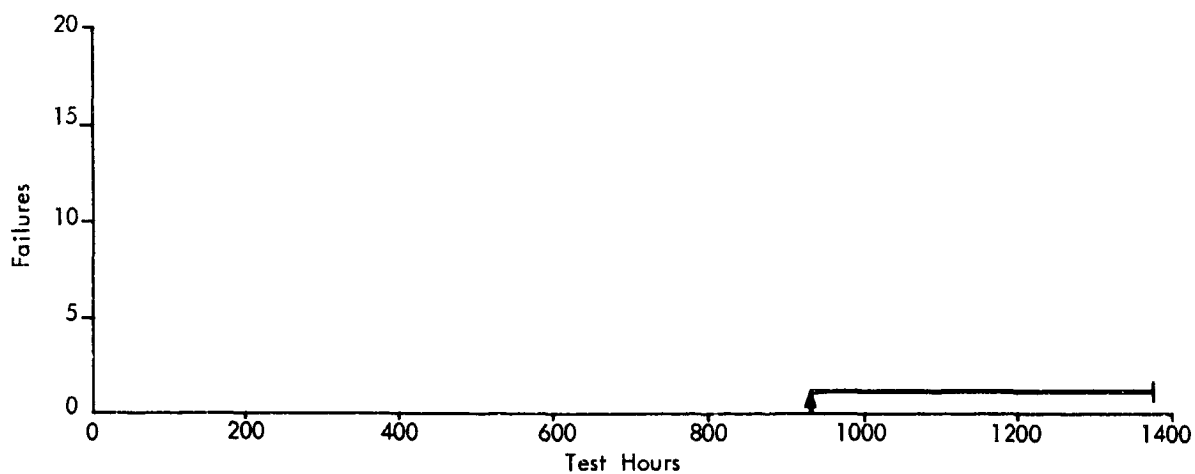


Figure 68. Phase II Module Failures ( >25 Millivolts) - Module No. 216

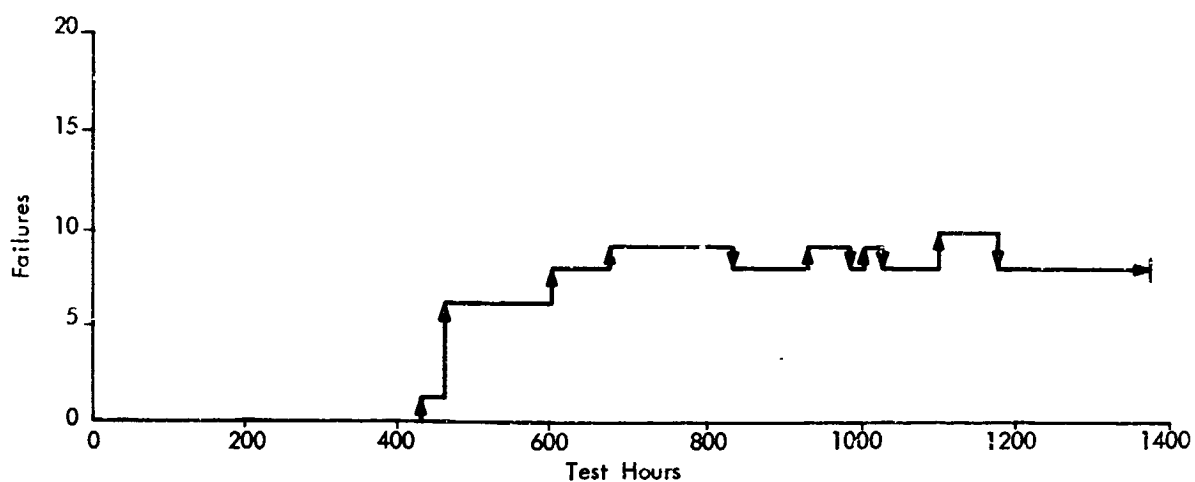


Figure 69. Phase II Module Failures ( >25 Millivolts) - Module No. 230

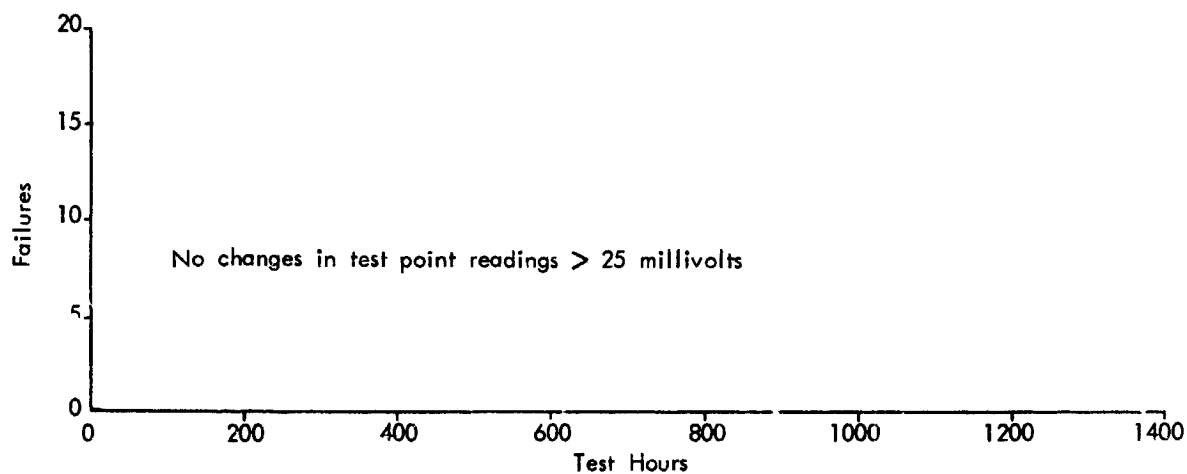


Figure 70. Phase II Module Failures ( >25 Millivolts) - Module No. 231

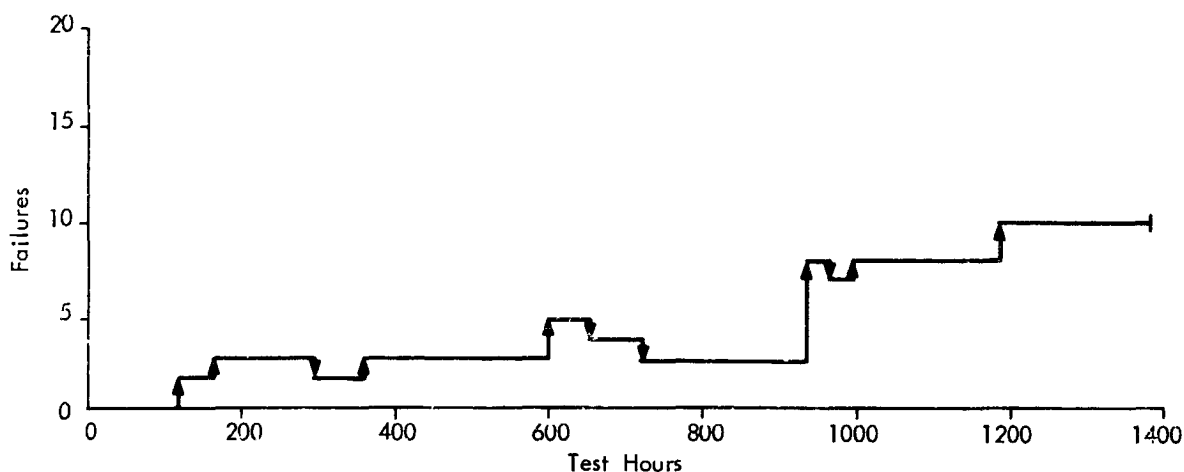


Figure 71. Phase II Module Failures (>25 Millivolts) - Module No. 232

the logic located internally on the module pages (away from the edges where the frame is deteriorating).

#### 4.5.2 Physical Examination

The nine representative replaceable modules were examined at the start of the Phase II testing period for defects in the materials or for any unusual physical characteristics. Particular attention was given to the RTV sealing compound and its adhesion to the magnesium-lithium module frame, to the adhesion of the silicone gasket to the female connector, and to the pin contacts. No defects or unusual characteristics (such as discolorations) were noted.

Figure 73 in the Appendix is a photograph of the nine modules under test conditions (photographed through the plexiglass test chamber) taken 9 days after the start of test. The photograph shows the beginning of an accumulation of salts and contaminants on the aluminum test fixture indicating the severity of the test. Figure 74 in the Appendix

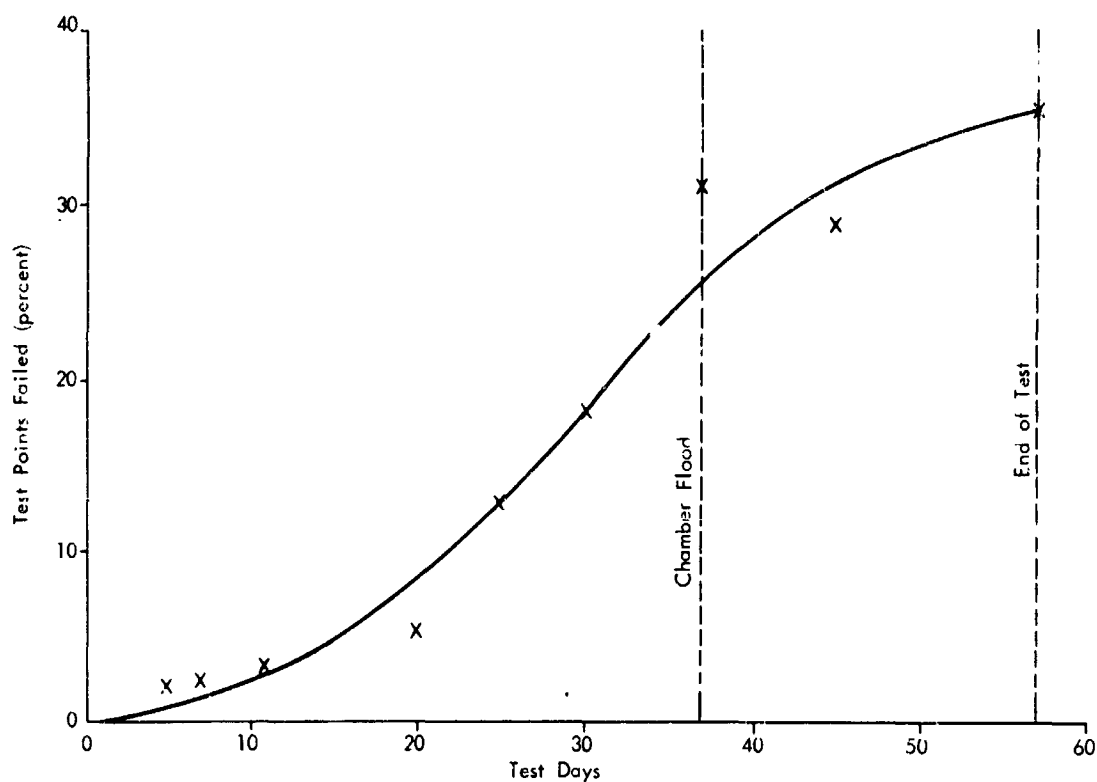


Figure 72. Summary of "Failures"

shows the same test fixture photographed out of the test chamber after 27 days of continuous testing.

Figure 75 shows seven of the nine modules removed from the test fixture after 27 days of testing. The two modules not shown could not be removed from the test fixture because of adhesive corrosion between the module frames and the fixture guides. The deterioration of the frames of the seven modules shown is noticeable, especially of Module 212 (middle right hand of photograph).

The test chamber failed 32 days after start of the test. Eight modules were removed from the chamber and test fixture at this time and photographed. Difficulty was experienced in removing several of the modules from the fixture because of adhesive corrosion, and one module could not be removed. Photographs of the eight individual modules are shown in Figures 76 through 83, which are in the Appendix.

Testing of Module 212 had to be discontinued at this time because its circuits began to draw excessive current. Figure 84 in the Appendix shows an end view of the module and the peeling of the RTV caused by the deterioration of the frame. Note the pieces of foreign matter that have fallen between the RTV seal and the logic module. Appendix Figure 85 is an enlargement of one section of the module showing the exposure of the logic after loose RTV was cut away.

Although physical inspection of Module 212 indicated that the excessive current drawn by this module was probably due to a failure in the module sealing, the gasket attached to the female connector was also found to be loose (indicating that the connector might have contributed to the failure) as shown in Figure 86, in the Appendix.

In general, the contact pins were found to be in very good shape on all the modules at this time. Appendix Figure 87 is an enlargement of the set of pins exhibiting the worst pin discoloration. A chemical analysis of the corrosion products identified the blue-green material as copper chloride hydrate and the black material as copper chloride combined with a small amount of copper oxide. (No nickel barrier layer existed between the copper pins and the gold plating on these connectors).

At the end of test (57 days), seven of the eight remaining modules were removed from the fixture and again photographed individually. Module 215 could not be removed because of adhesive corrosion. The seven modules are shown in Appendix Figures 88 through 94.

#### 4.5.3 Conclusions

Although it was not possible to assign the failure mechanism (which caused a test point reading to change by more than 25 millivolts) to either the connector or to the logic module, the general correlation between frame deterioration and failure occurrence indicates that most of the failures were due to leakage of moisture and contaminants into the logic circuits rather than by means of the connectors. The failure

of the magnesium-lithium frames and resulting loosening of the RTV seal were not considered significant, since hermetically sealed modules would be used in the AES computer.

**PHOTOGRAPHIC APPENDIX**

**AES-EPO STUDY PROGRAM**



Figure 56. Completed Mockup

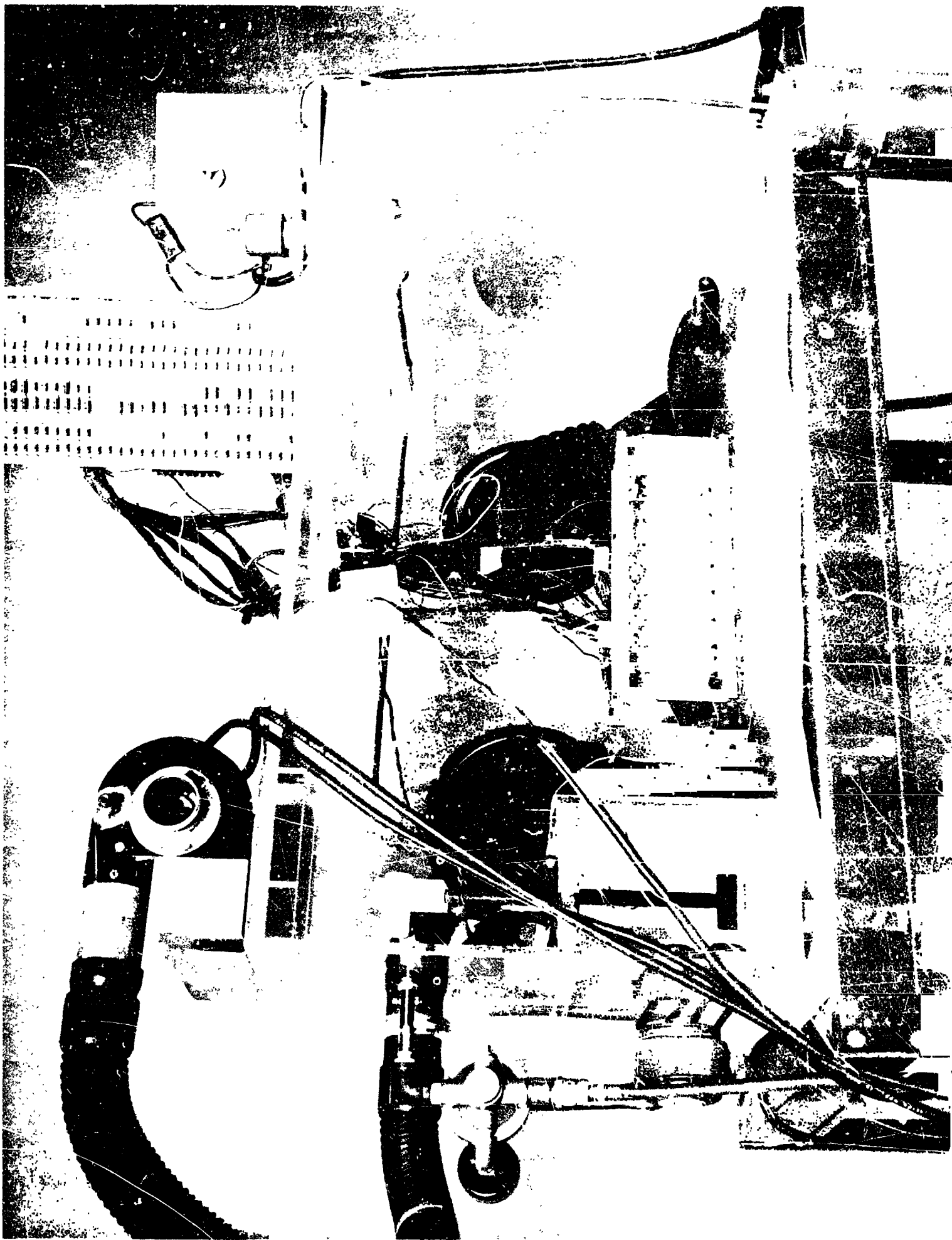


Figure 59. Environmental Test Chamber

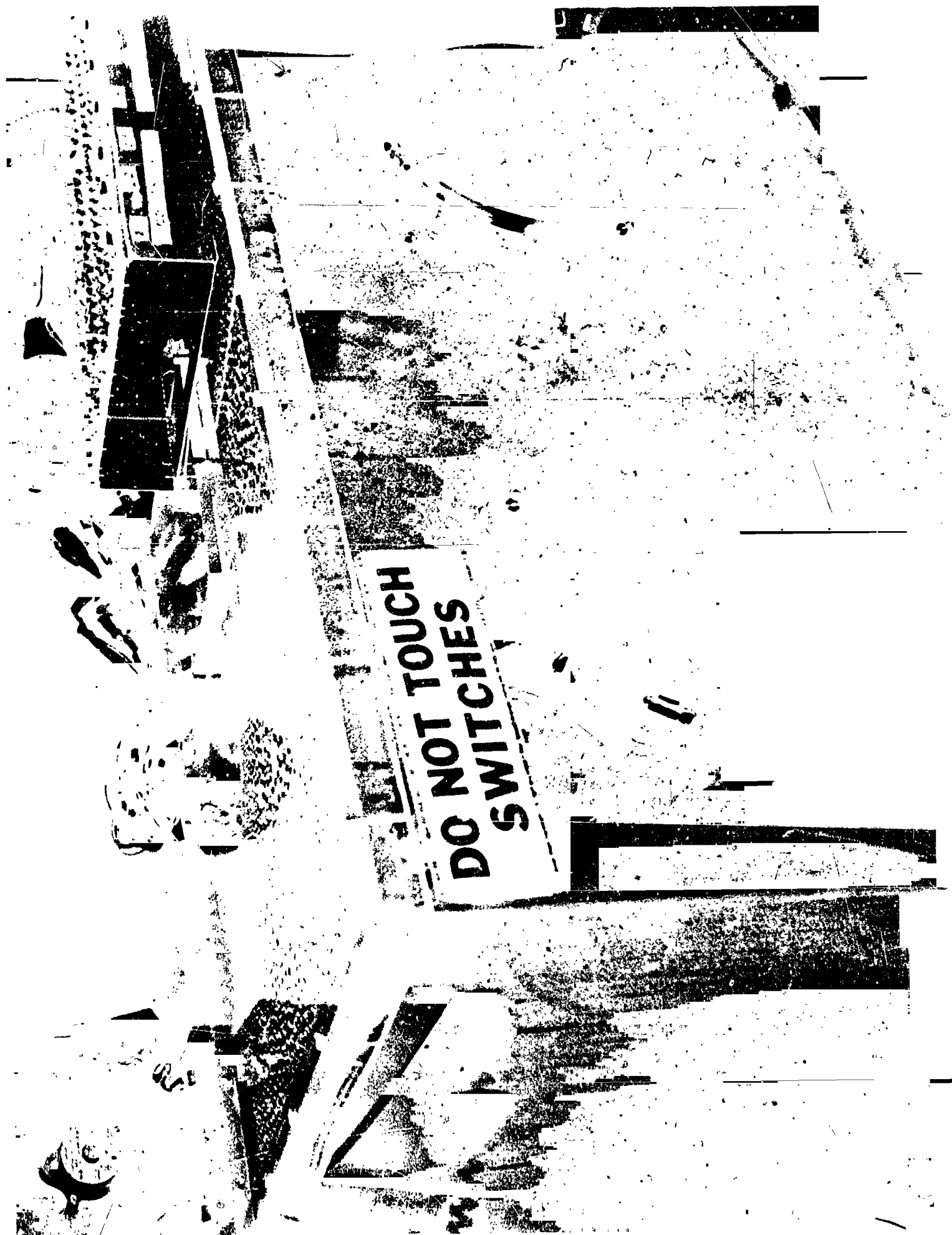


Figure 61. Chamber During Test

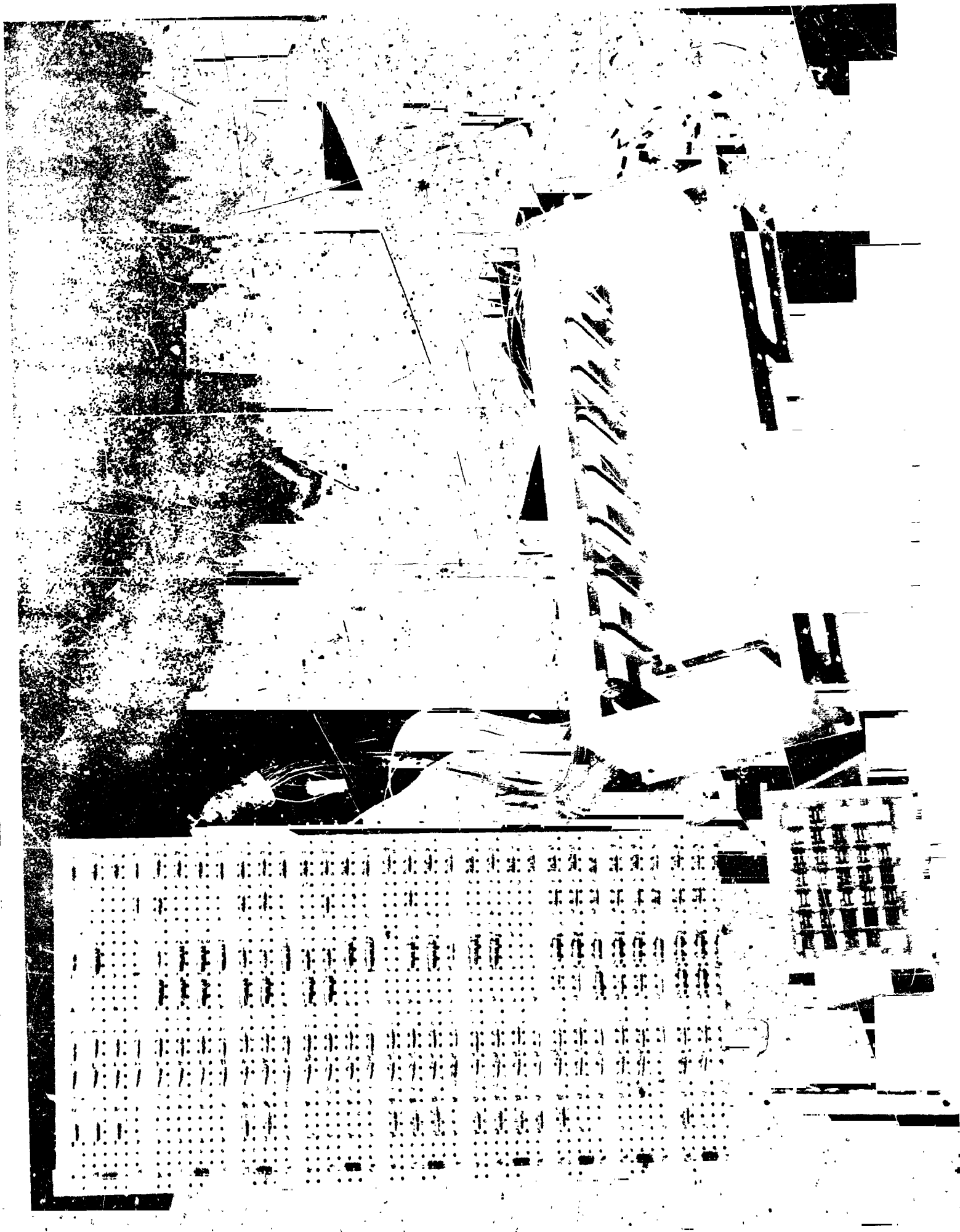


Figure 62. Test Fixture (Sheet 1 of 2)



Figure 62. Test Fixture (Sheet 2)



Figure 73. Nine Modules Under Test - 9 Days



Figure 74. Nine Modules Under Test - 27 Days

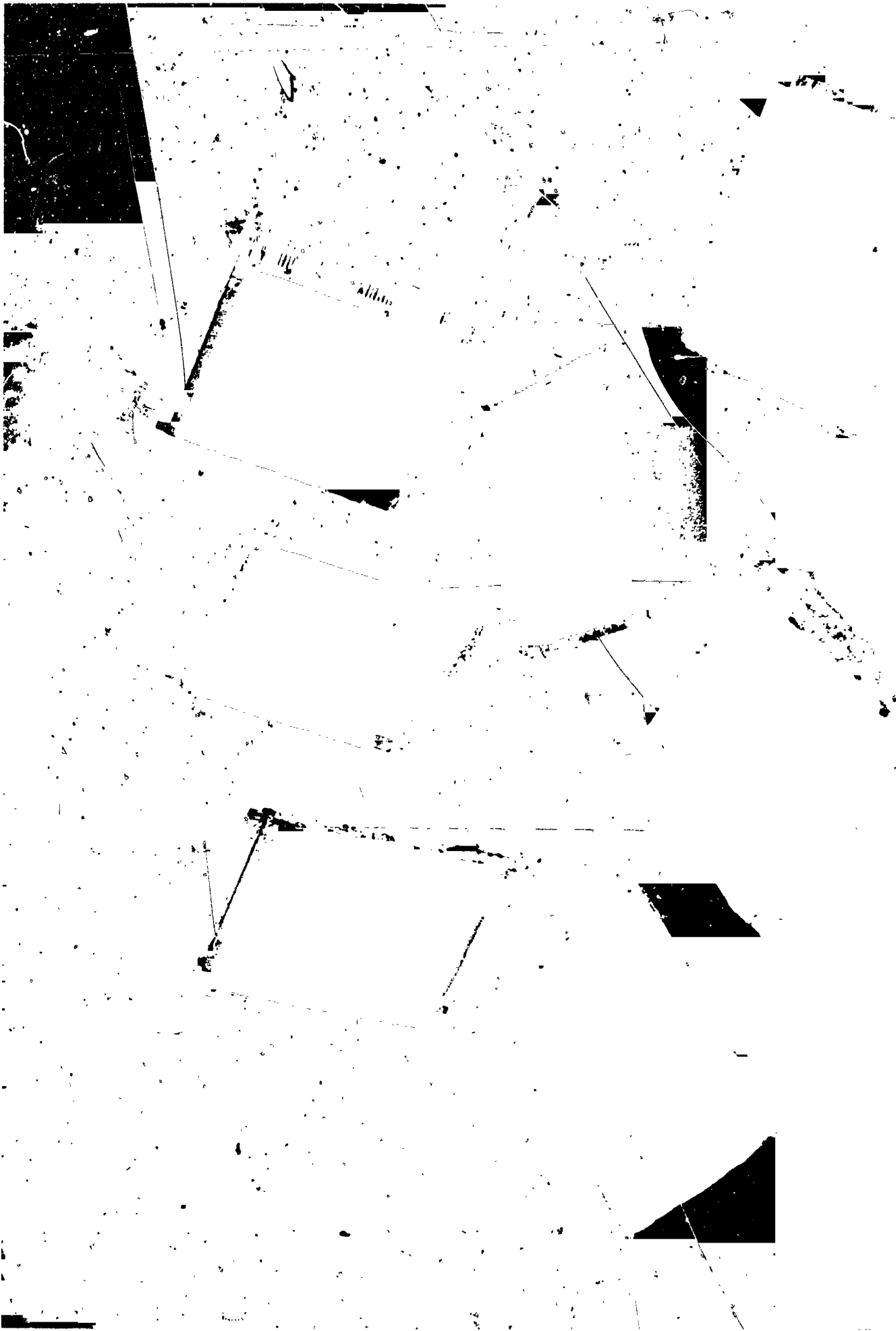


Figure 75. Seven Modules - 27 Days



Figure 76. Individual Module - 32 Days



Figure 77. Individual Module - 32 Days

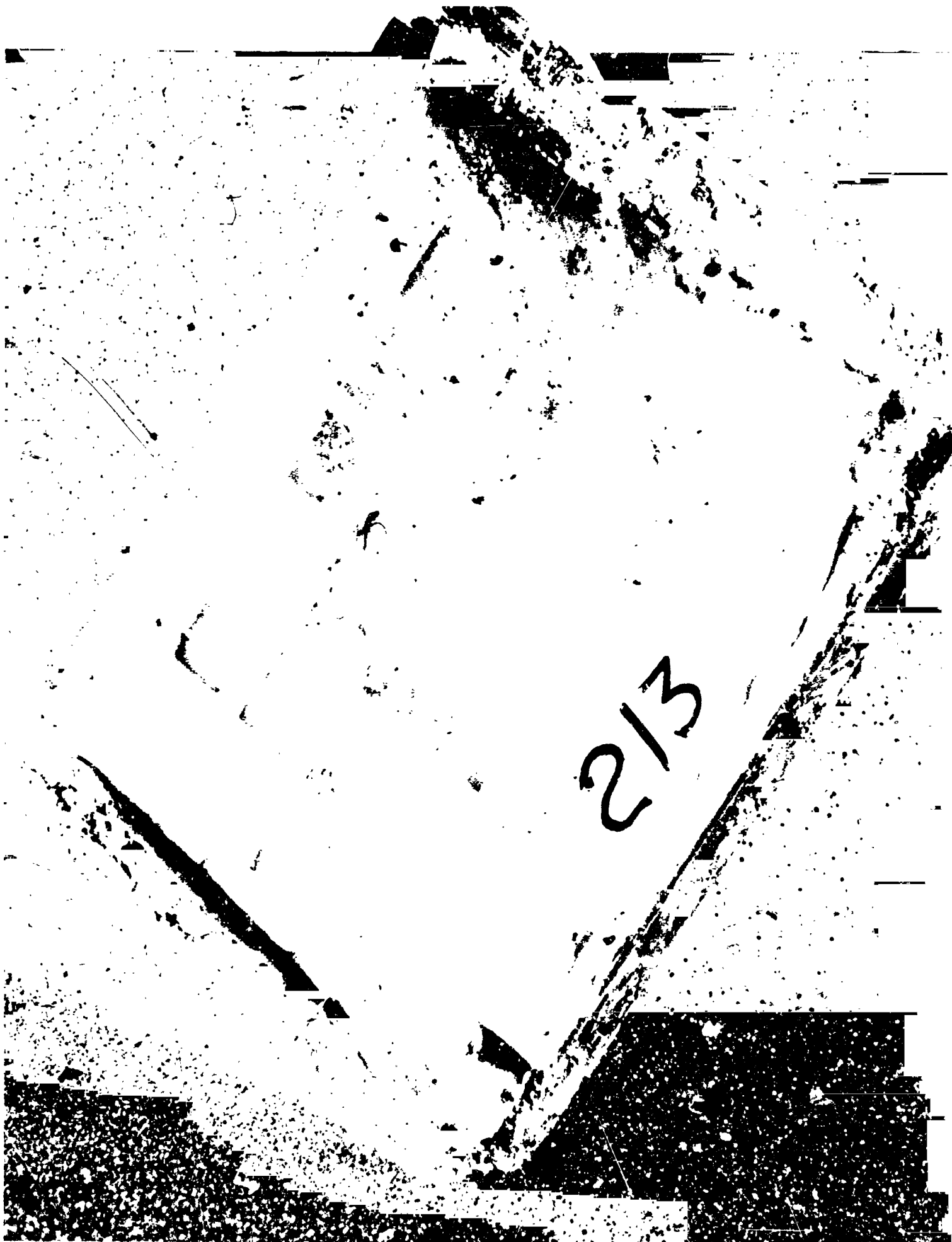


Figure 78. Individual Module - 32 Days

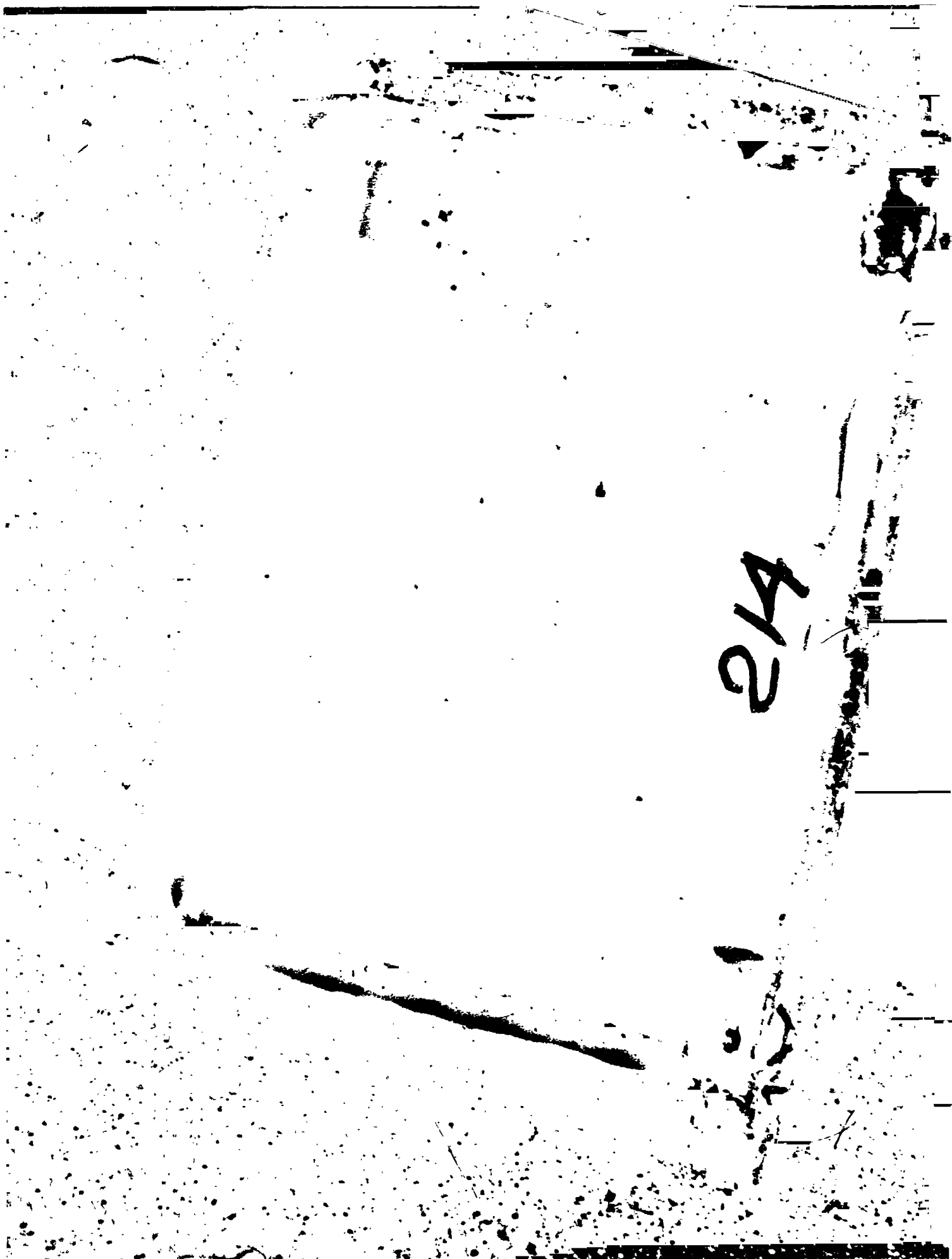


Figure 79. Individual Module - 32 Days



Figure 80. Individual Module - 32 Days



Figure 81. Individual Module - 32 Days

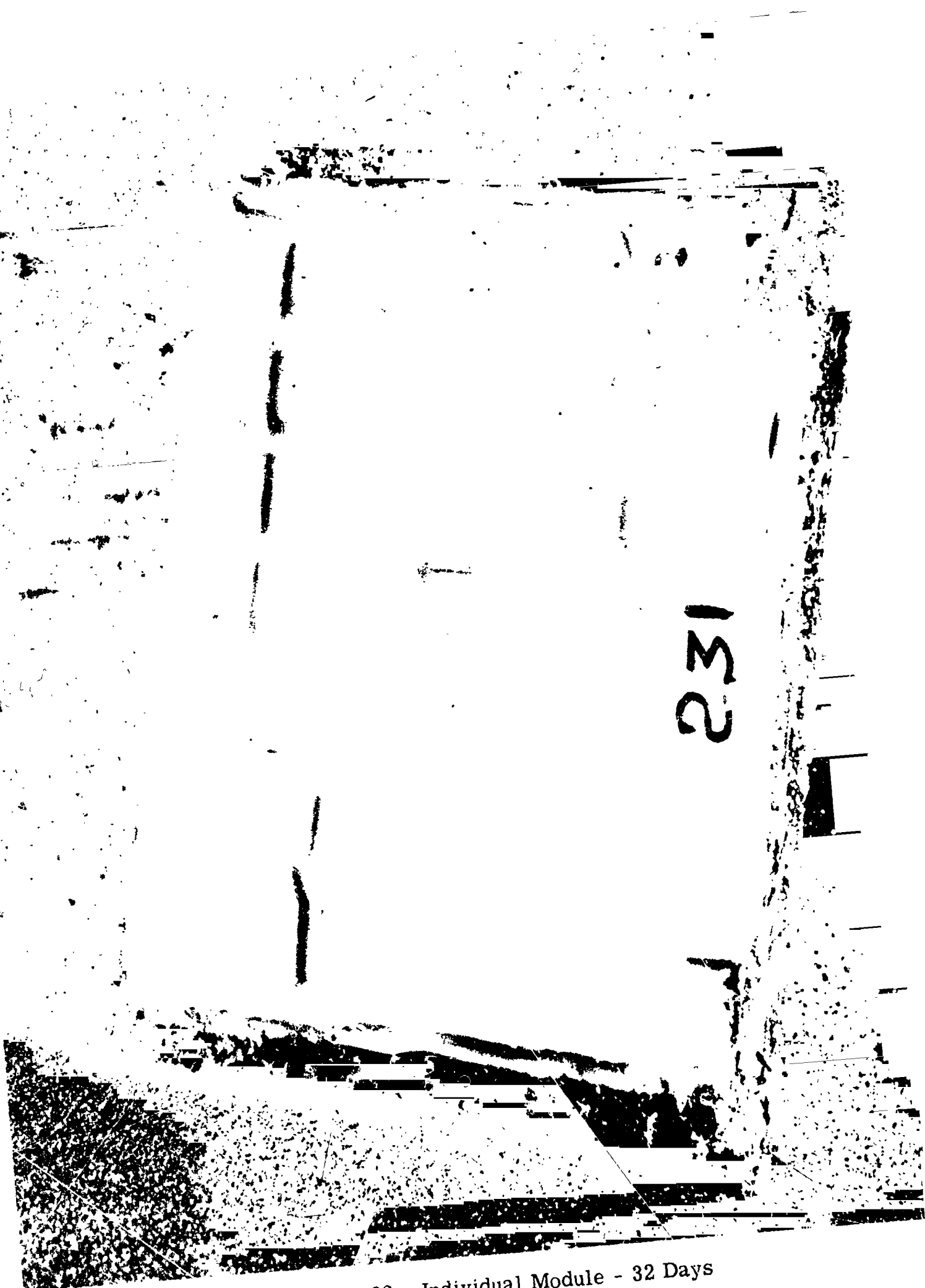


Figure 82. Individual Module - 32 Days



Figure 83. Individual Module - 32 Days

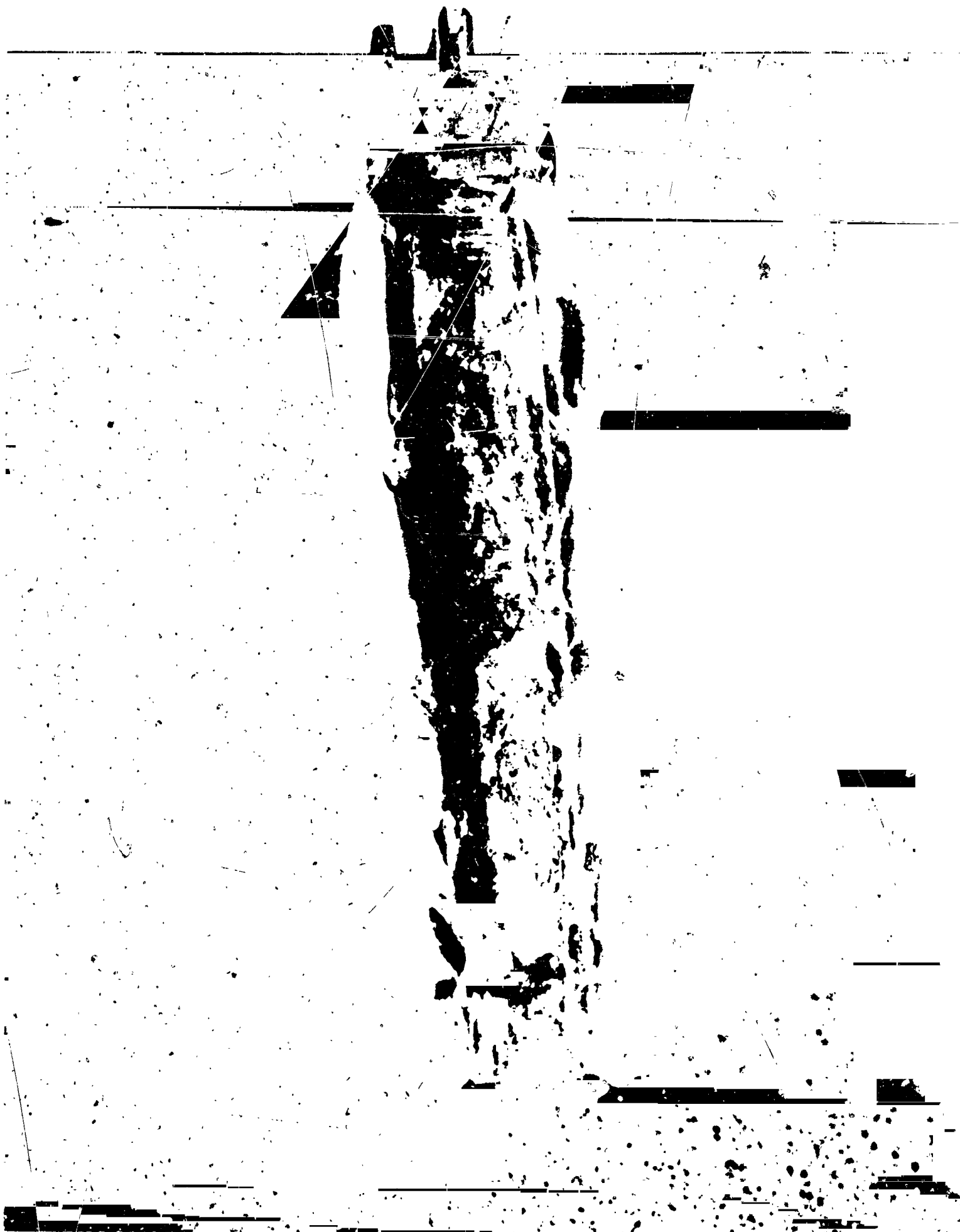


Figure 84. Module 212 - 32 Days

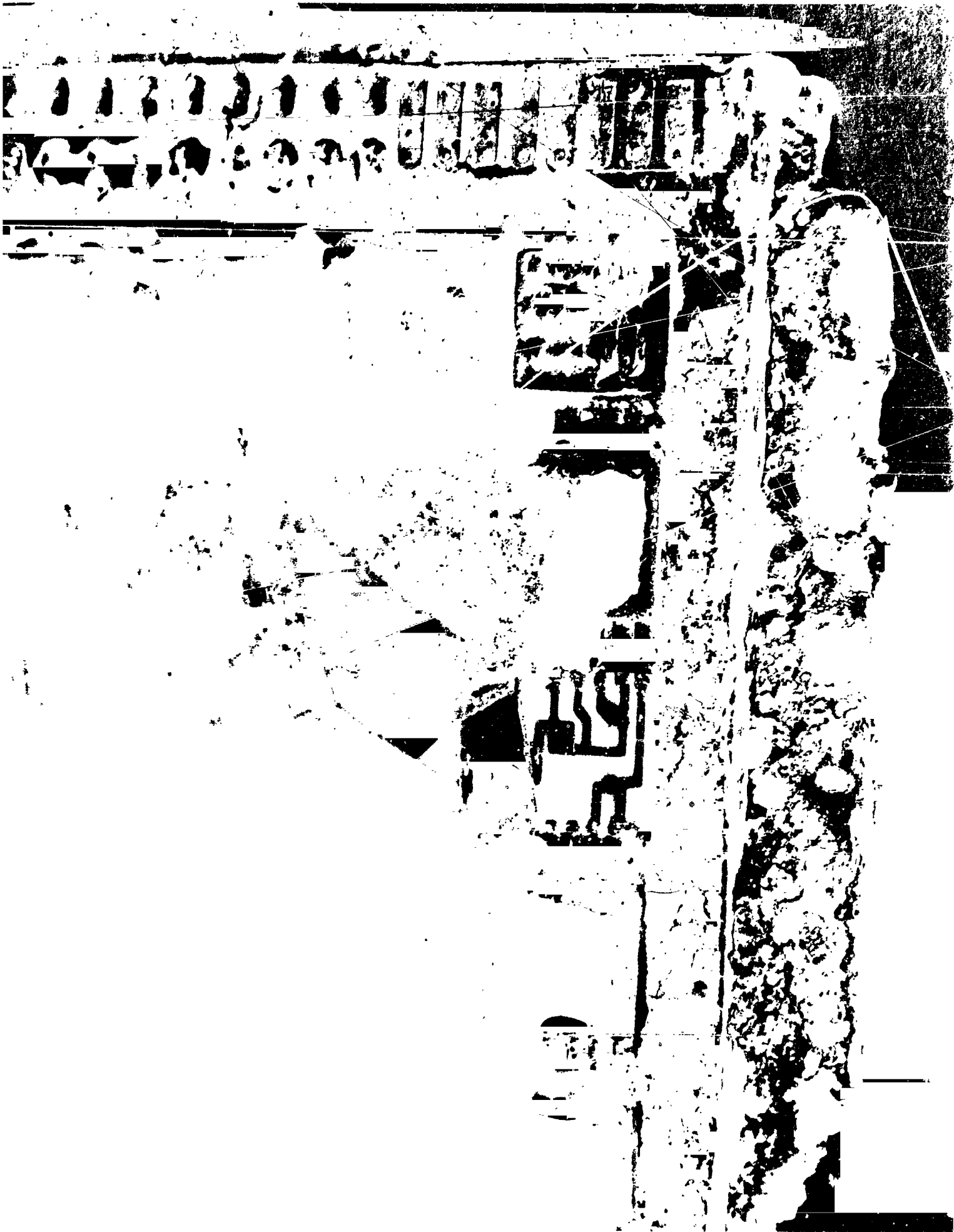


Figure 85. Module 212 Enlargement - 32 Days



Figure 86. Module 212 Female Connector - 32 Days

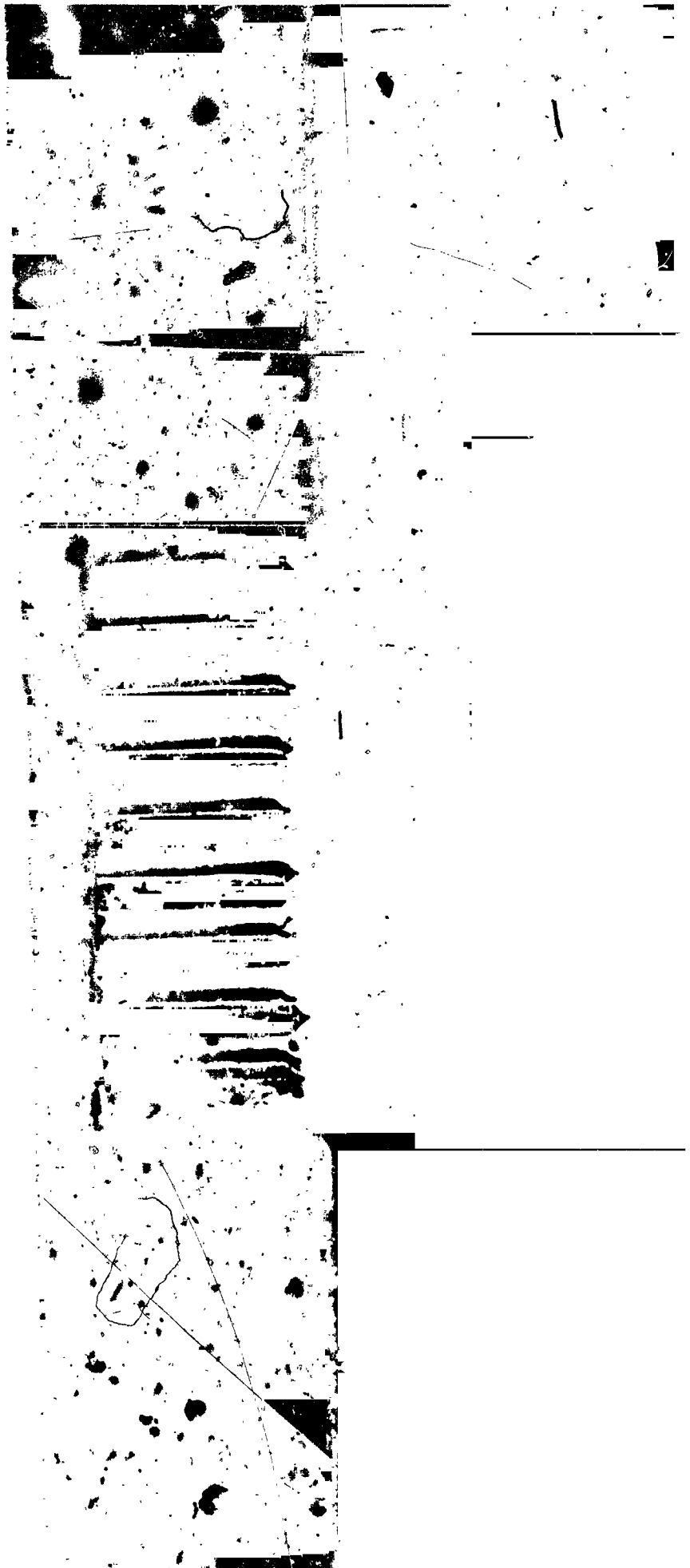


Figure 87. Module Pin Discoloration - 32 Days

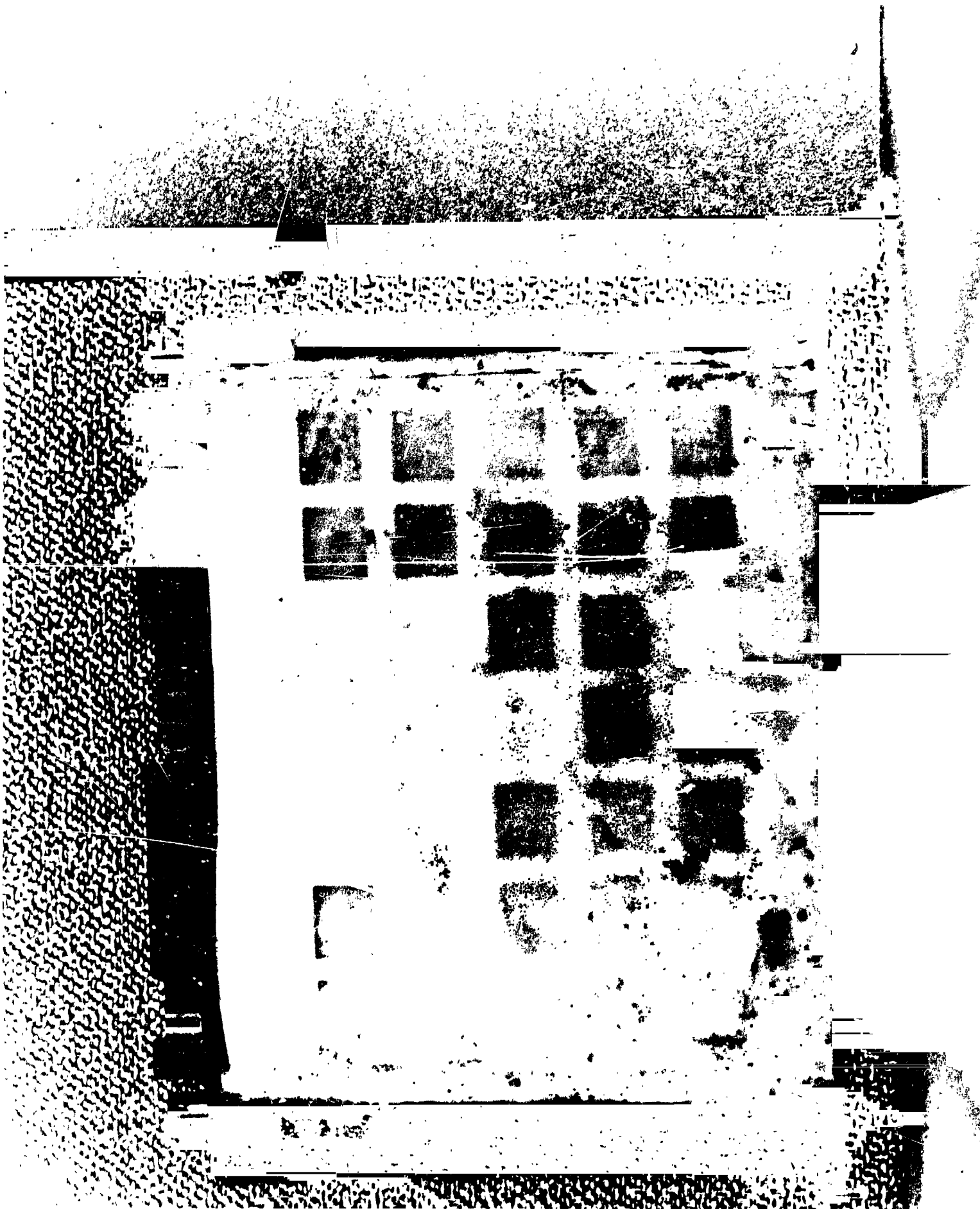


Figure 88. Individual Module - 57 Days

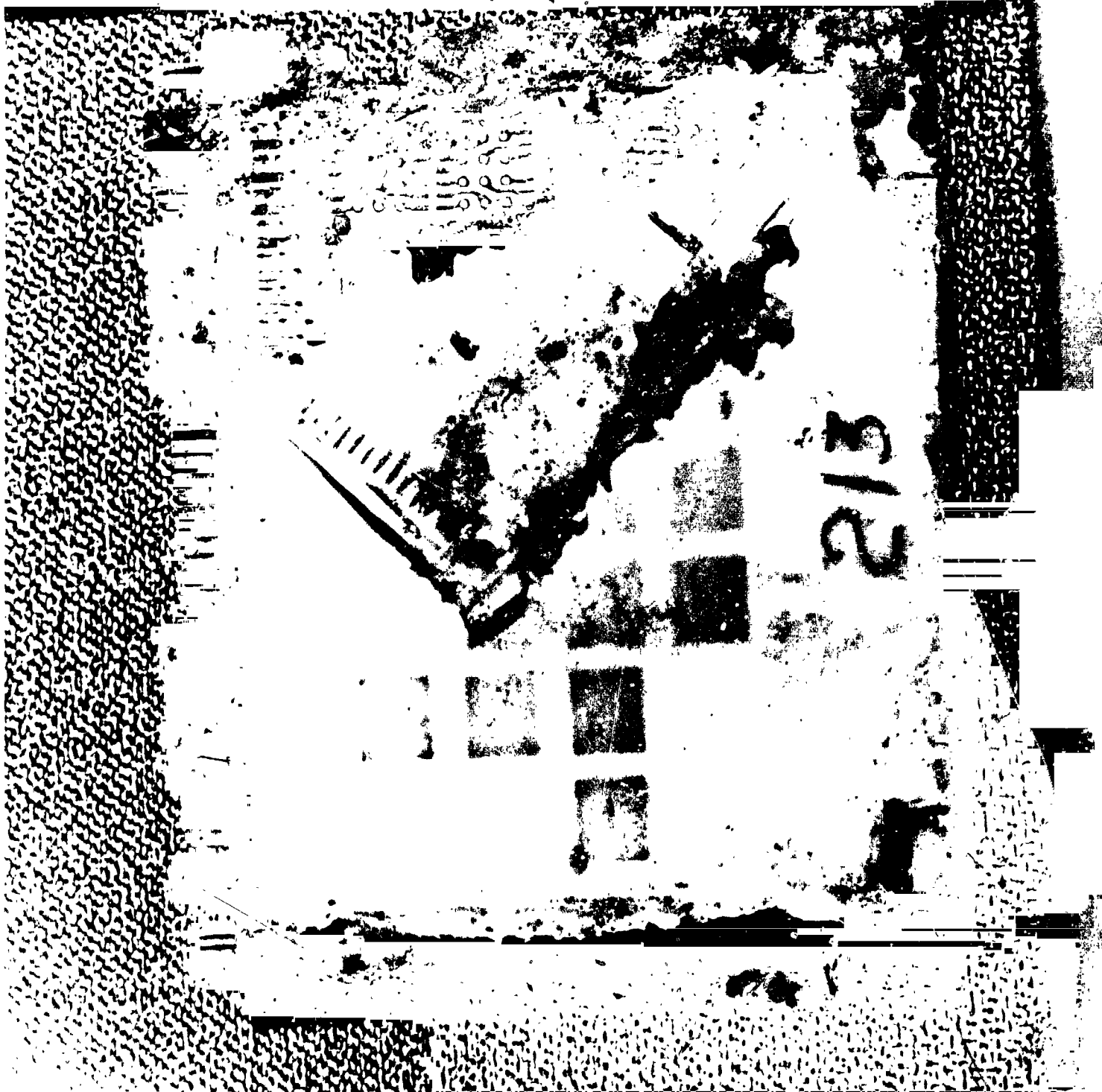


Figure 89. Individual Module - 57 Days

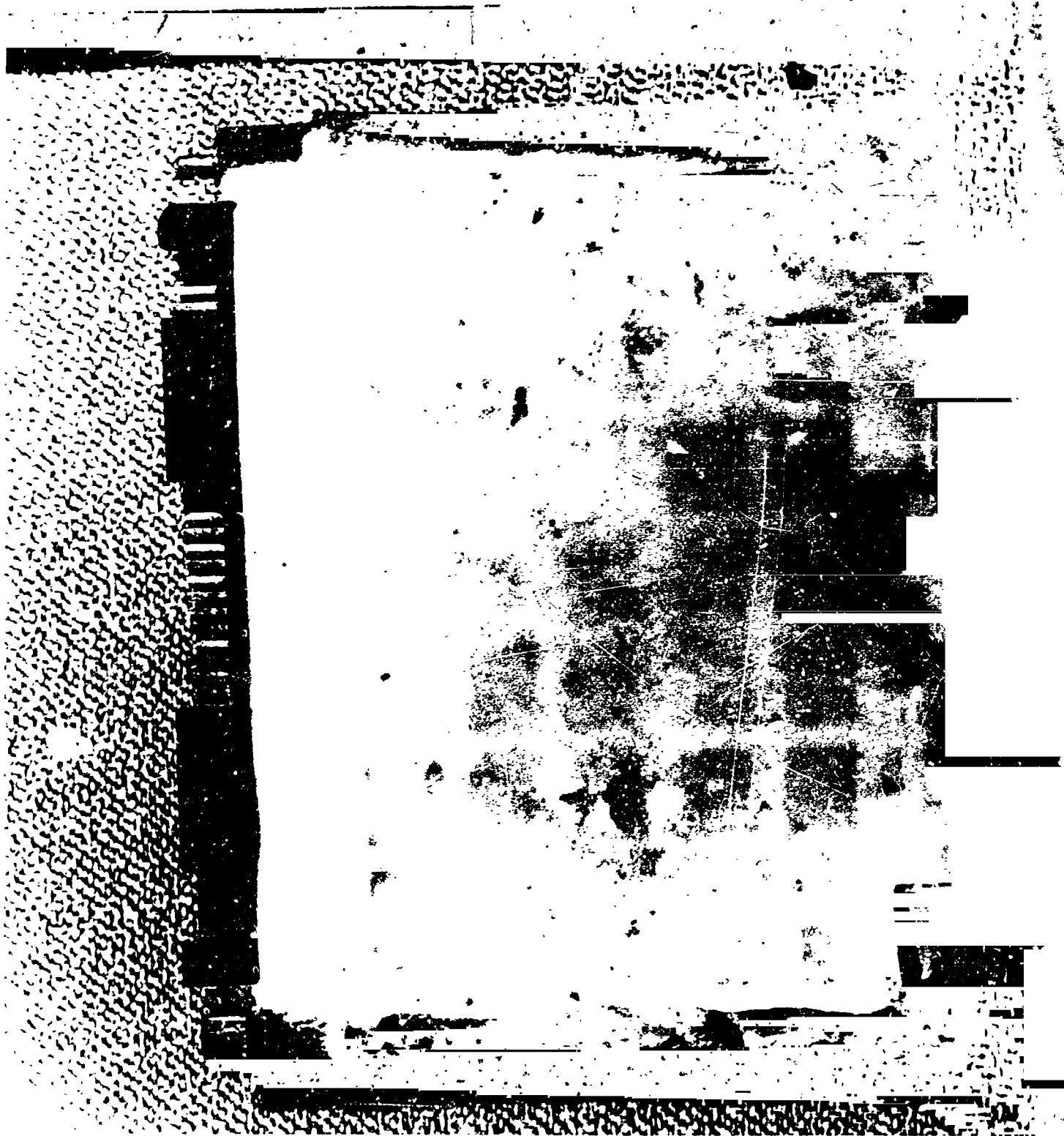


Figure 90. Individual Module - 57 Days

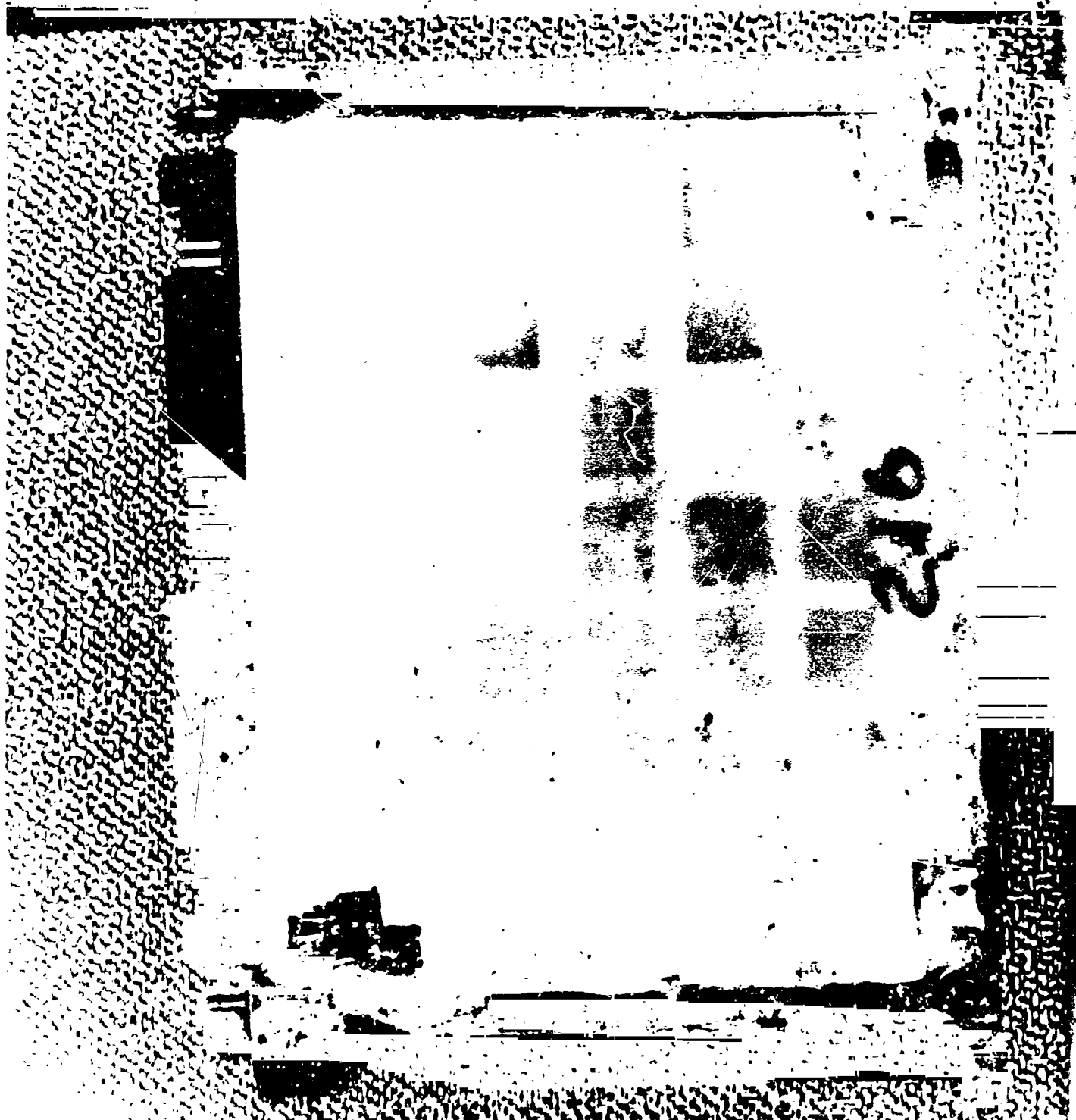


Figure 91. Individual Module - 57 Days

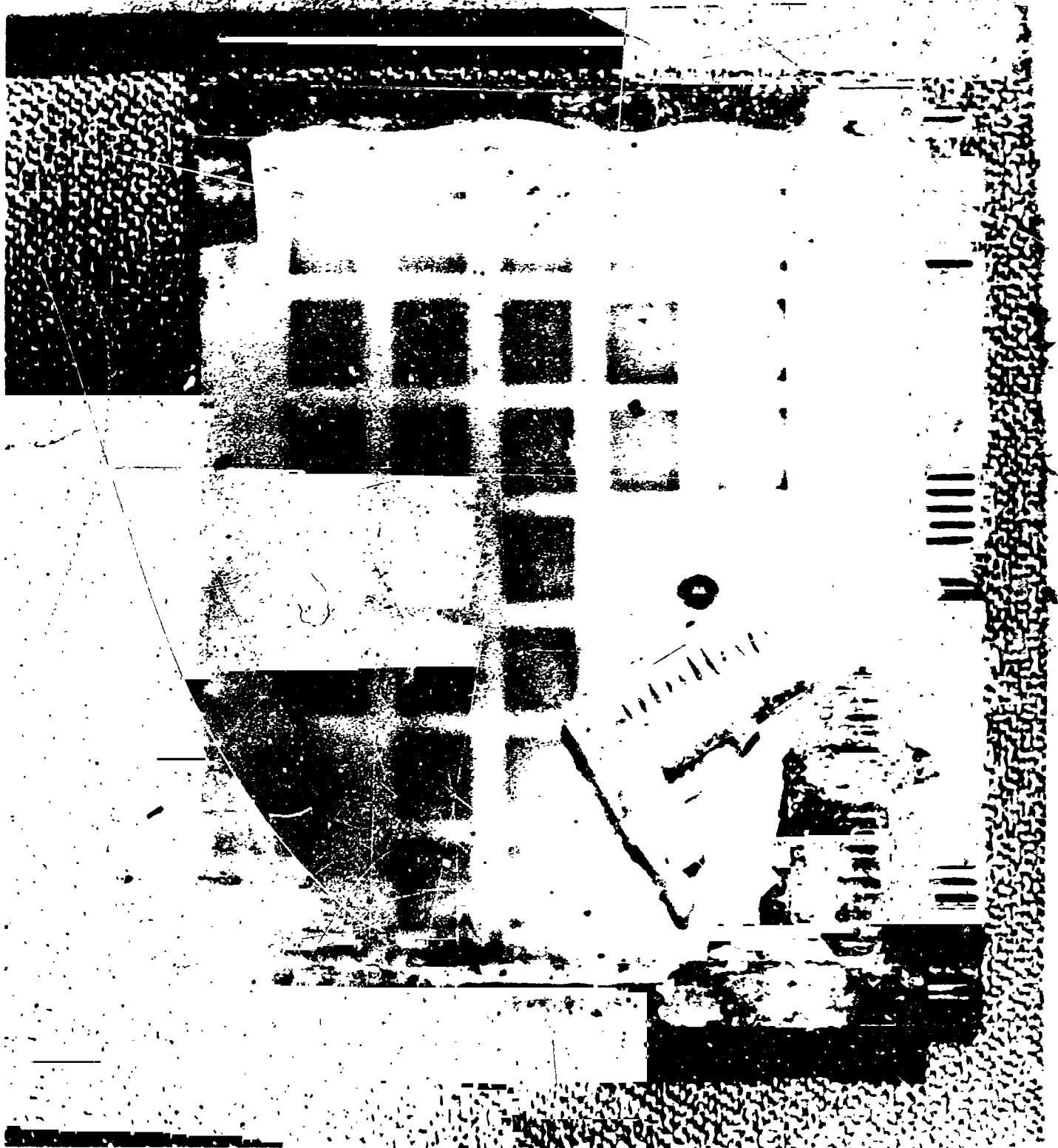


Figure 92. Individual Module - 57 Days

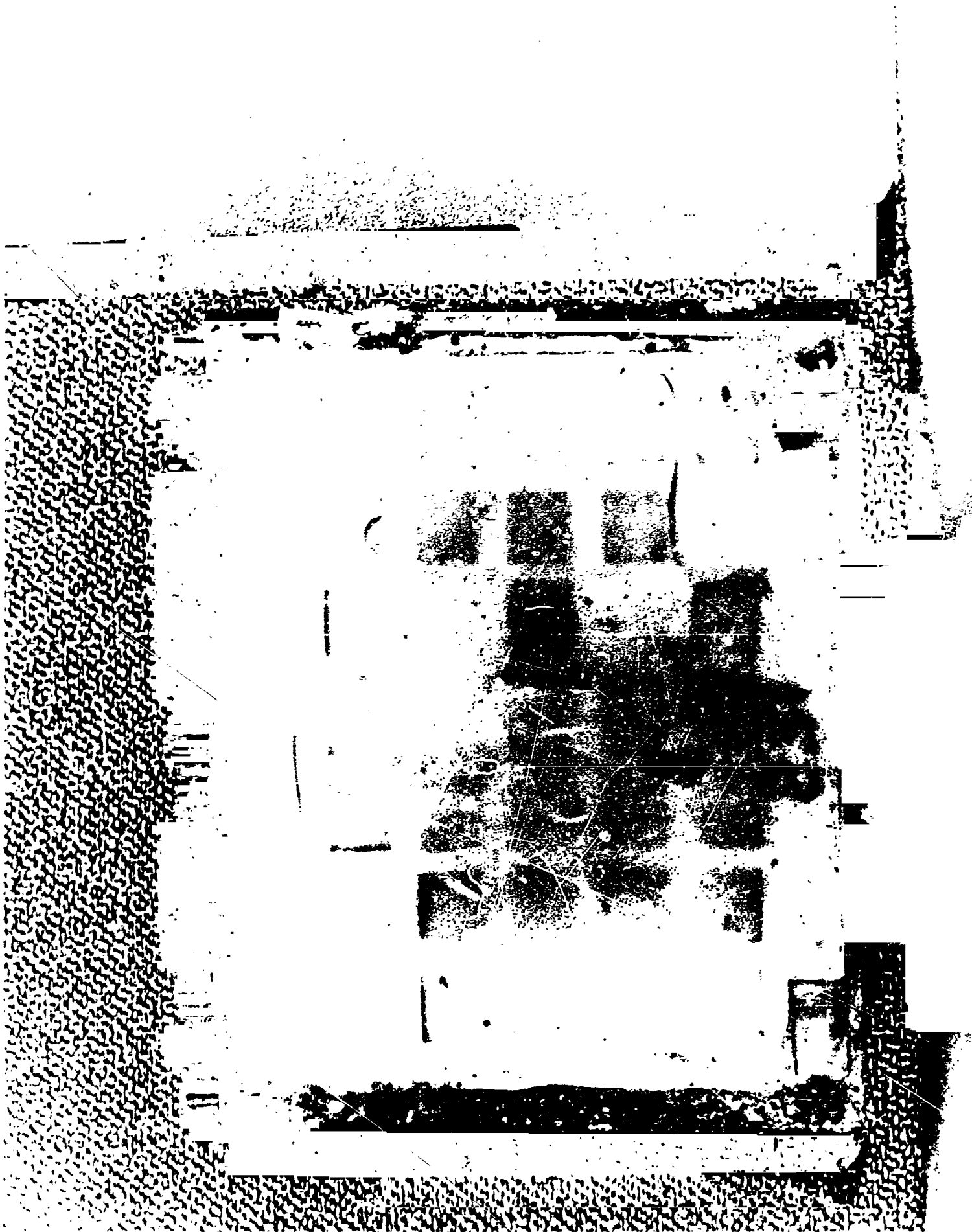


Figure 93. Individual Module - 57 Days

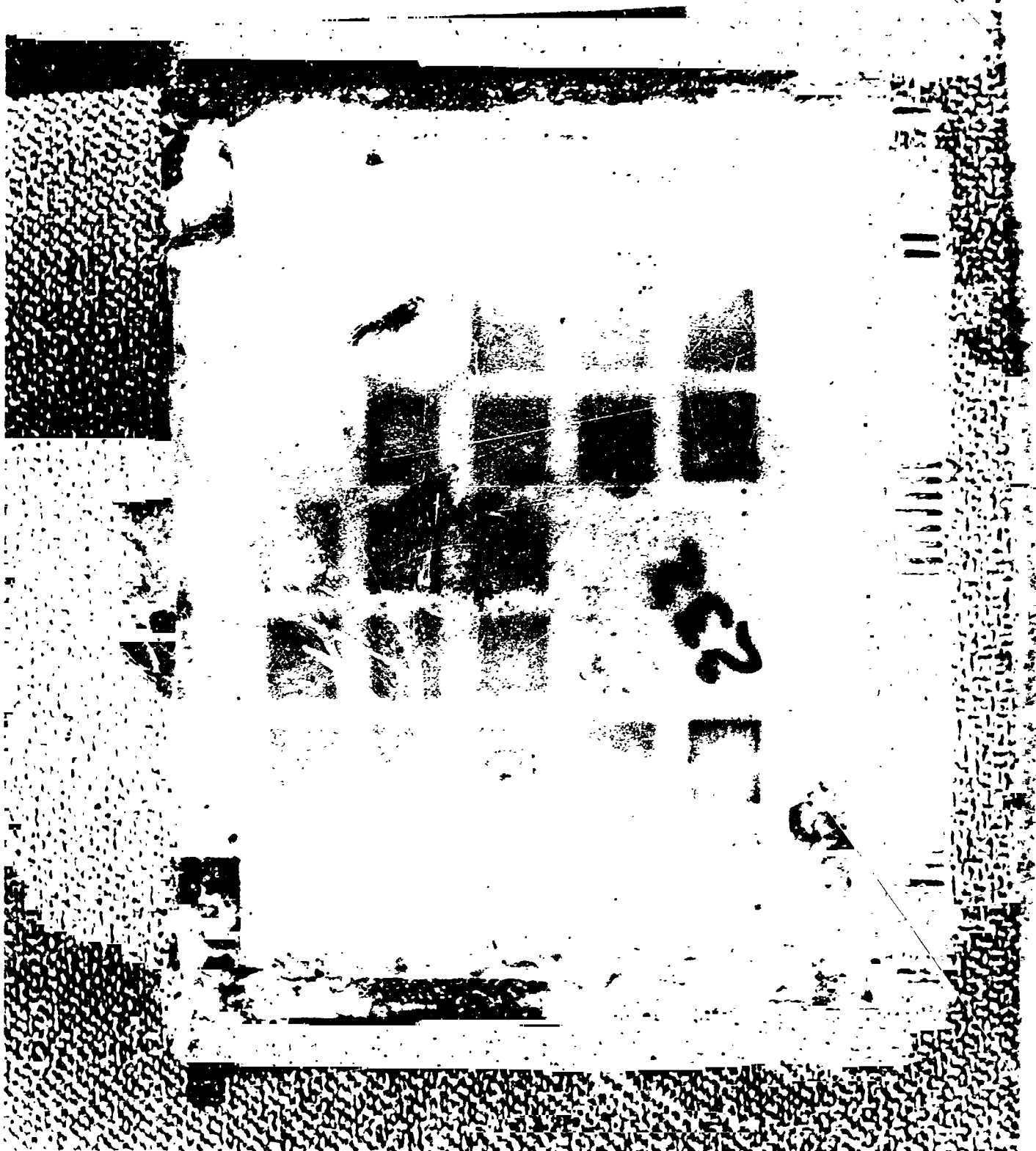


Figure 94. Individual Module - 57 Days